ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В ЦИФРОВОМ МИРЕ

СБОРНИК НАУЧНЫХ ТРУДОВ

Под редакцией
доктора юридических наук,
заслуженного юриста Российской Федерации
В.С. Овчинского

Москва
ИНФРА-М
2021

УДК 343.98
ББК 67.52
О60

Сборник подготовлен при поддержке
Всероссийской полицейской ассоциации МПА

О60 **Оперативно-розыскная деятельность в цифровом мире** : сборник научных трудов / под ред. В.С. Овчинского. — Москва : ИНФРА-М, 2021. — 630 с.

ISBN 978-5-16-017227-9

Межведомственный сборник статей посвящен актуальным проблемам использования форм и методов оперативно-розыскной деятельности в условиях бурного распространения инновационных технологий. Особое внимание уделено вопросам кибербезопасности, возможностям искусственного интеллекта, методологическим проблемам оперативно-розыскной деятельности в цифровом мире, применения новых технологий на наиболее острых направлениях борьбы с преступностью и обеспечения безопасности.

Материалы сборника будут полезны ученым и практическим работникам системы правоохранительных органов, студентам, курсантам юридических вузов и факультетов, всем интересующимся проблемами обеспечения безопасности и борьбы с преступностью в период новой технологической революции.

УДК 343.98
ББК 67.52

ISBN 978-5-16-017227-9

© Коллектив авторов, 2021

Оглавление

От редактора. Цифровизация, преступность, оперативно-розыскная деятельность: угрозы и возможности 7

РАЗДЕЛ I. КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМЕ ОПЕРАТИВНО-РОЗЫСКНОЙ, РАЗВЕДЫВАТЕЛЬНОЙ И КОНТРРАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

О транснациональном характере современной киберпреступности и задачах по противодействию ей со стороны субъектов оперативно-розыскной деятельности (*П.П. Городов*) 24

Кибервойна с кибермошенниками: антифрод Сбербанка России и взаимодействие с оперативными подразделениями МВД России и ФСИН России (*С.К. Кузнецов*) 30

Кибермафия как объект оперативно-розыскного воздействия (*Ю.Н. Жданов, В.С. Овчинский*) 36

О значении общих признаков «криминального» и «государственного» кибертерроризма для оперативно-розыскной, разведывательной и контрразведывательной деятельности (*Е.Н. Яковец*) 48

Координация деятельности спецслужб в киберзащите государства: опыт Израиля (*Е.С. Ларина, В.С. Овчинский*) 72

РАЗДЕЛ II. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

Перспективные направления использования искусственного интеллекта в оперативно-розыскной деятельности (*И.Л. Хромов, Н.А. Кузьмин, И.А. Завьялов*) 94

Хакатон «Искусственный интеллект на службе полиции» (*В.В. Агеев*) 104

О некоторых научных проблемах использования искусственного интеллекта в оперативно-розыскной деятельности (*А.А. Бабушкин, А.А. Маслов, В.С. Овчинский*) 108

РАЗДЕЛ III. МЕТОДОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ТЕОРИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ЦИФРОВОМ МИРЕ

Цифровизация общества и виртуализация реальности: усложнение вызовов и расширение перспектив оперативно-розыскной деятельности (*А.Л. Осипенко*) 150

К вопросу о сущности и содержании оперативно-розыскного мероприятия «получение компьютерной информации» (*Е.Н. Яковец*) 173

Формирование системы оперативно-розыскного контроля органов внутренних дел за лицами, склонными к совершению преступлений, в условиях развития информационного общества (*А.А. Бабушкин*) 190

О необходимости введения в научный оборот оперативно-розыскной категории «дистанционное мошенничество» (*С.И. Давыдов, Е.О. Наливайко*) 201

Цифровые платформы оперативно-розыскной профилактики преступлений (*А.С. Овчинский*) 212

О перспективах развития розыскной и идентификационной деятельности в условиях цифровизации общества (*А.В. Парфёнов*) 246

Полемика о концептуальных основах цифровой оперативно-розыскной деятельности (*Ю.А. Лапунова, А.Ю. Бегунов*) 255

Особенности подготовки аналитиков для подразделений, осуществляющих информационно-аналитическое обеспечение оперативно-розыскной деятельности органов внутренних дел Российской Федерации (*Г.Г. Саркисян*) 261

Возможности видеонаблюдения для оперативно-розыскной деятельности (*Ю.Н. Жданов, В.С. Овчинский*) 269

Оперативно-розыскное обеспечение коллективной безопасности в условиях информационного общества (*А.А. Маслов*) 292

РАЗДЕЛ IV. ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ НА ОСНОВНЫХ НАПРАВЛЕНИЯХ БОРЬБЫ С ПРЕСТУПНОСТЬЮ

Актуальные вопросы оперативно-розыскной деятельности по борьбе с незаконным наркопроизводством в современной России в условиях цифровой реальности (*А.В. Морозов*) 312

Современное состояние оперативно-розыскного противодействия преступлениям экономической и коррупционной направленности с использованием информационно-коммуникационных технологий (*Р.Г. Искалиев, А.В. Телков*) 328

К вопросу об использовании информационно-коммуникационных технологий для защиты бюджетных средств, выделяемых на реализацию национальных проектов (программ) (*А.В. Телков*) 336

Цифровые технологии в оперативно-розыскной деятельности уголовного розыска по противодействию организованной преступности (*П.В. Эзрохин*) 346

К вопросу об использовании данных, полученных в ходе оперативно-розыскной деятельности органов внутренних дел в сети Интернет, в борьбе с организованной преступностью (*А.В. Воронцов*) 357

Инновационные технологии в комплексе оперативно-розыскного противодействия торговле людьми (*В.И. Коваленко*) 365

Международное сотрудничество в борьбе с транснациональной организованной преступностью и терроризмом: специальные методы расследования, электронные доказательства, цифровые технологии (*Ю.Н. Жданов, В.С. Овчинский*) 403

Стратегия Евросоюза по борьбе с организованной преступностью на 2021–2025 годы и ее значение для совершенствования оперативно-розыскной деятельности в цифровой среде (*Ю.Н. Жданов, В.С. Овчинский*) 428

Развитие насыщающего террора в форме скулшутинга и задачи оперативных подразделений (*И.Ю. Сундиев*) 450

Оперативно-розыскная характеристика использования технологии геймификации в экстремистской и террористической деятельности (*И.Ю. Сундиев, А.А. Смирнов*)..... 455

Цифровой экстремизм и его значение для оперативно-розыскной деятельности (*М.А. Кочубей, А.А. Смирнов*) 473

О знании тенденций развития правых движений на Западе и их цифровом обеспечении для организации работы оперативных подразделений Российской Федерации (*А.А. Смирнов*)..... 498

Терроризм и технологии XXI века: что должно быть под контролем оперативных подразделений? Европейский взгляд (*В.С. Овчинский*)..... 548

Приложение. Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (проект) 563

Сведения об авторах 623

Список сокращений 626

Всероссийская полицейская ассоциация МПА 627

Посвящается памяти
Константина Константиновича Горяинова,
Валерия Михайловича Атмажитова,
Валерия Павловича Кувалдина

От редактора
ЦИФРОВИЗАЦИЯ, ПРЕСТУПНОСТЬ, ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ: УГРОЗЫ И ВОЗМОЖНОСТИ

В XXI в. цифровая трансформация стала ключом к формированию экономической и социальной устойчивости, а также глобального влияния. Общее будущее человечества уже обретает форму в цифровой сфере. В мире, где ведется геополитическая конкуренция за технологическое первенство, необходимо гарантировать, что цифровая революция будет опираться на принципы открытого общества, верховенства закона и фундаментальных свобод.

Пандемия COVID-19 ускорила переход к цифровой экономике, которая станет ключом к будущему росту и возможностям. Мобильные устройства, интернет, облачные вычисления и другие инновации создали гиперсвязанное глобальное пространство, в котором миллиарды людей могут работать и вести более динамичный образ жизни. Цифровые платформы изменили то, как мы потребляем, работаем и создаем экономическую ценность, а цифровые активы, такие как компьютеры, коммуникационное оборудование и программное обеспечение, помогли компаниям снизить производственные затраты и повысить эффективность.

Цифровая трансформация будет продолжать ускоряться с более широким внедрением больших данных и конвергенцией технологий Четвертой промышленной революции, таких как 5G, искусственный интеллект (ИИ) и «Интернет вещей». Уже *Глобальный опрос McKinsey* обнаружил, что пандемия побудила компании ускорить «оцифровку взаимодействия с клиентами и цепочками поставок, а также своих внутренних операций на три-четыре года».

Но вопрос в том, распространятся ли выгоды от этого ускорения за пределы бизнеса — на работников и потребителей? Из-за того, что старые технологии, процессы и даже целые отрасли становятся устаревшими, цифровизация будет и дальше приводить к потере рабочих мест (*Ли Джонг-Ва. Построение инклюзивного цифрового будущего. 08.06.2021, PS*).

Всемирный экономический форум 2020 в Отчете о будущем рабочих мест предсказывает, что многие частные компании будут использовать машины и алгоритмы более широко, чем когда-либо, что затрудняет перспективы трудоустройства в различных секторах

и регионах. Роботы, ИИ и другие новые технологии могут стать угрозой для 15% сотрудников средней компании уже к 2025 г.

С учетом таких эффектов цифровая трансформация может усилить социальное и экономическое неравенство и увеличить разрыв в заработной плате между квалифицированными и неквалифицированными работниками.

Эти социальные факторы являются питательной средой для разного уровня конфликтов, которые могут перерасти в акты криминальной агрессии, экстремизма, терроризма, торговли людьми, массовую незаконную миграцию.

Цифровая революция также вызывает политические проблемы, например, когда правительства и корпорации злоупотребляют данными и технологиями. Во время вспышки COVID-19 некоторые страны использовали приложения для отслеживания контактов, данные о мобильности, камеры и другие цифровые технологии для сдерживания вируса, но это наблюдение часто происходило за счет конфиденциальности. Из-за того что технологические гиганты обладают такой огромной властью благодаря управлению пользовательскими данными, потребители все больше осознают важность ***безопасности данных и защиты конфиденциальности***.

Большинству стран потребуется политика, направленная на сокращение разрыва в цифровых навыках и доступе, поскольку для увеличения доли рабочих мест потребуется больше технологических ноу-хау. Системы образования должны делать больше, чтобы вооружить учащихся знаниями и навыками, которые им понадобятся в цифровом будущем. А профессиональная подготовка должна способствовать тому, чтобы все сотрудники были в курсе последних цифровых технологий.

Когда речь идет о больших технологиях, правила и стандарты доцифровой экономики больше не применяются, а это означает, что большинству стран потребуется обновить свою политику в области конкуренции и нормативно-правовую базу.

Попутно они должны установить ***более четкие правила и стандарты для безопасности данных, владения цифровыми технологиями и конфиденциальности пользователей***.

В 2020 г. в Европе начали активно разрабатывать следующий этап инновационного прорыва. Речь уже идет о начале реализации концепции ***Индустрия 5.0.***

Обновленная европейская Индустрия 5.0, по замыслу разработчиков, должна сделать отрасли более ориентированными на будущее, устойчивыми и ориентированными на человека.

Концепция Индустрии 5.0 обсуждалась в 2020 г. на ряде форумов участниками из научно-исследовательских и технологических организаций. Были определены ***шесть категорий***, каждая из которых, как считается, раскрывает свой потенциал в сочетании с другими, как часть технологических структур:

1) индивидуализированное взаимодействие человека и машины;

2) биоинформационные технологии и интеллектуальные материалы;

3) цифровые двойники и моделирование;

4) технологии передачи, хранения и анализа данных;

5) искусственный интеллект;

6) технологии энергоэффективности, возобновляемых источников энергии, хранения и автономии.

Индустрия 5.0 уходит корнями в концепцию Индустрии 4.0, которая была разработана в Германии в 2011 г. как будущий проект и часть стратегии страны в области высоких технологий. Она была направлена на лучшее соответствие не только экономическим, но и особым экологическим требованиям «зеленого производства» для углеродно-нейтральной и энергоэффективной промышленности.

Реализация правительственной инициативы «Сделано в Китае 2025» напрямую вдохновлена «Индустрией 4.0», направленной на оживление китайской обрабатывающей промышленности и обеспечение плавного перехода.

За 10 лет своего существования Индустрия 4.0 уделяла меньше внимания исходным принципам социальной справедливости и устойчивости и больше внимания — цифровизации и технологиям, основанным на ИИ, для повышения эффективности и гибкости производства.

Индустрия 5.0 напрямую связана с Концепцией «Общество 5.0». Обе концепции относятся к фундаментальному сдвигу общества и экономики в сторону новой парадигмы. Концепция Общества 5.0 была представлена ***важнейшей бизнес-федерацией Японии «Кейданрен»*** в 2016 г. Впоследствии ее продвигало ***правительство Японии***. Япония, по сути, встраивает аспекты цифровизации, главным образом на уровне отдельных организаций и частей общества, в полноценную национальную стратегию трансформации, политику и даже философию.

В концепции ***«Общества»*** способ, которым люди обеспечивают себе средства к существованию, напрямую связан с тем, как они строят свое общество. Нумерация до ***«5»*** является результатом совсем другого и гораздо большего временного масштаба, чем у про-

мышленных революций. Первые два «Общества» соответствуют доиндустриальным периодам (до конца XVIII в.) и связаны соответственно с охотой/собирательством и сельским хозяйством. Общество 3.0 является индустриальным обществом и более или менее соответствует периоду первой, второй и частично третьей промышленных революций. Общество 4.0 характеризуется преобладанием «информации», оно эволюционировало от сильно оцифрованной версии третьей промышленной революции до сегодняшнего дня. ***Общество 5.0 пытается сбалансировать экономическое развитие с решением социальных и экологических проблем.*** Оно не ограничивается производственным сектором, но решает более серьезные социальные проблемы, основанные на интеграции физического и виртуального пространств. ***Общество 5.0 — это общество, в котором передовые ИТ-технологии, «Интернет вещей», роботы, ИИ и дополненная реальность активно используются в повседневной жизни, промышленности, здравоохранении и других сферах деятельности, в первую очередь не для экономической выгоды, а для выгоды и удобства каждого гражданина.***

С цифровизацией связаны и ***серьезные риски, в числе которых тотальная слежка, кибератаки на критически важную инфраструктуру, распространение дезинформации, поляризация общества, подрыв демократии***. Все это означает, что надо искать баланс между открытостью и остальными важнейшими интересами и ценностями.

Национальный совет по разведке (США) в своем новом ***докладе «Глобальные тенденции — 2040»*** прогнозирует, что в ближайшие десятилетия противоречия в мире будут только усиливаться. В докладе отмечено, что в течение следующих двух десятилетий темпы и влияние технологических достижений, вероятно, увеличатся, трансформируя и улучшая человеческий опыт и возможности и предлагая потенциал для решения таких проблем, как старение, изменение климата и низкий рост производительности, ***создавая при этом новую напряженность*** и сбои внутри и между сообществами, отраслями промышленности и государствами.

Сверхсвязанный мир — это будущее, которое уже начинает появляться. Сети следующего поколения, постоянные датчики и бесчисленные технологии будут объединены в глобальную систему с миллиардами подключенных устройств. Например, сегодняшние повсеместные общедоступные камеры приведут к появлению ***умных городов завтрашнего дня, в которых оптические и другие дат-***

чики объединяются с ИИ для наблюдения за людьми, транспортными средствами и инфраструктурой во всем мире.

По некоторым оценкам, нынешний «Интернет вещей», предшественник гиперподключенного будущего, достигнет 64 млрд объектов к 2025 г. по сравнению с 10 млрд в 2018 г., и все они будут отслеживаться в режиме реального времени.

Если заглянуть в будущее, то мир с гиперподключениями может поддерживать до 1 млн устройств на квадратный километр с помощью систем сотовой связи следующего поколения (5G) по сравнению с 60 тыс. устройств, которые в настоящее время возможны с текущими сотовыми сетями, с еще более быстрыми сетями на горизонте. Сетевые датчики станут повсеместными.

В 2020 г. работало более 20 млрд устройств, а с появлением новых наземных сетей в сочетании с увеличением количества космических услуг прогнозируется, что ***сотни миллиардов, а в конечном счете и триллионы устройств могут быть подключены во всем мире***.

Конфиденциальность и анонимность могут фактически исчезнуть по выбору или по поручению правительства, поскольку все аспекты личной и профессиональной жизни отслеживаются глобальными сетями.

Созданные в реальном времени или ***синтетические СМИ могут еще больше искажать правду и реальность, дестабилизируя общество с такой скоростью и в таких масштабах, которые затмевают нынешние проблемы дезинформации***.

Многие виды преступлений, особенно те, которые можно отслеживать и пресекать с помощью цифрового наблюдения, станут менее распространенными, в то время как ***могут возникнуть новые преступления и потенциально новые формы дискриминации***.

Расширение возможностей подключения почти наверняка ***повысит уязвимость подключенных к сети людей, организаций и правительств, поскольку наличие сотен миллиардов подключенных устройств значительно увеличивает поверхность киберфизических атак.***

Созрели условия как для более широкого международного сотрудничества, так и ***для новых типов многогранной конкуренции и конфликтов***, которые могут определить наступающую эру.

Темпы технологических изменений могут ***усилить социальную напряженность между теми, у кого есть доступ, способность и желание адаптироваться, и теми, кто не может или не хочет меняться***. Благодаря быстрому распространению и вне-

дрению технологий некоторые люди, сообщества и страны могут быстро развиваться, в то время как другие могут остаться без надежды наверстать упущенное, что усугубит неравенство внутри государств и между ними. Внедрение технологий также может опережать этическую зрелость и регулирование, создавая ***потенциально разрушительную социальную тревогу и политические разногласия***. Эти противоречия могут еще больше усилиться за счет использования искусственно созданных сообщений или сообщений, предназначенных для ИИ, таких как глубокие подделки.

Будущее, насыщенное технологиями и связанное с гиперсвязью, предложит лидерам и правительствам новые инструменты для мониторинга своего населения, что позволит улучшить предоставление услуг и безопасность, но также предложит более ***широкие средства контроля***. Те же технологии, которые позволяют гражданам общаться, организовывать и контролировать свое здоровье, предоставляют все большие объемы данных правительствам и частному сектору.

Технологический прогресс может увеличить количество экзистенциальных угроз. Эти угрозы могут нанести ущерб жизни в глобальном масштабе, они бросают вызов нашей способности представить и понять их потенциальные масштабы, и они требуют разработки устойчивых стратегий для выживания. Технологии играют роль как в создании этих рисков для существования, так и в их смягчении. ***Антропоморфные риски включают безудержный ИИ, искусственные пандемии, нанотехнологическое оружие или ядерную войну.*** Такие маловероятные события со значительными последствиями трудно прогнозировать и к ним дорого готовиться, но заблаговременное выявление потенциальных рисков и разработка стратегий смягчения могут обеспечить некоторую устойчивость к экзогенным шокам.

Такое «светлое будущее» прогнозирует всему человечеству, а значит и гражданам России, американский Национальный совет по разведке.

Технологическая готовность к противоборству становится главнейшим элементом развития страны.

При этом следует соблюдать ***три главных принципа: равное игровое поле на цифровых рынках, безопасность в киберпространстве, свобода в онлайне*** (в том числе защита свободы слова и собраний, а также защита от дискриминации и от вмешательства в личную жизнь).

Целью усилий государства и общества будет ***достижение человеко-ориентированной цифровой трансформации, которая***

позволит получить максимальные выгоды от технологий и минимизировать создаваемые ими риски.

В киберпространстве, как и в физическом мире, Россия выступает за базовые глобальные ценности. «Всеобщая декларация прав человека» 1948 г. провозгласила такими ценностями достоинство человека, свободу слова и убеждений, право на невмешательство в личную жизнь и на отсутствие дискриминации. Важно гарантировать, чтобы цифровая революция соответствовала этим принципам.

Особая ответственность за реализацию этих принципов лежит на государственных органах, уполномоченных осуществлять ***оперативно-розыскную деятельность (ОРД)*** в ходе борьбы с преступностью и обеспечения безопасности.

ОРД является наиболее острым оружием в руках государства по сдерживанию негативных социальных явлений. ***Преступность, терроризм, коррупция, отмывание денег все в большей мере становятся цифровыми. Одновременно сама ОРД уже в большой мере стала цифровым инструментом борьбы с перечисленными явлениями.***

Можно выделить несколько наиболее перспективных направлений использования ОРД в ходе цифровой трансформации.

Первое. Киберпандемия

Термин «киберпандемия» родился не сейчас. Еще в 2016 г. антивирусная лаборатория «PandaLabs» компании «Panda Security» опубликовала «белую книгу» о «киберпандемии» — компьютерных атаках в сфере здравоохранения.

Пандемия коронавируса придала этому термину новое звучание. ***Под киберпандемией понимается возможность втягивания человечества в киберконфронтацию и даже кибервойну. Проявлениями киберпандемии являются хакерство, кибертерроризм, кибервмешательство в частную жизнь и развитие государств.***

Сюда же относится и то, что ряд государств провозглашают доктрины права на нанесение так называемых упреждающих кибердударов даже по потенциальному противнику, когда ничья вина еще не доказана.

С начала марта 2020 г. в условиях карантина и мер самоизоляции в мире наблюдается ***беспрецедентный глобальный рост вредоносной киберактивности***. Фишинговые атаки, направленные на кражу денег или секретов у работников домашнего офиса, более чем удвоились по сравнению с прошлым годом, а в некоторых местах они выросли многократно. Было также предпринято несколько попыток кибератак на критически важную ин-

фраструктуру, включая аэропорты, электросети, порты и объекты водоснабжения и канализации. Даже больницы, в которых лечат пациентов с COVID-19, стали мишенью, и Всемирная организация здравоохранения сообщила о пятикратном увеличении количества атак на ее сети.

Обеспокоенность вызывает ***обвальный рост киберпреступности в России*** (до 510,4 тыс. преступлений по итогам 2020 г., +74%), обусловленный введением режима самоизоляции и переходом многих компаний на удаленный режим работы (через сеть Интернет). Удельный вес таких деяний в общей структуре преступности увеличился с 14,5 до 25%. Как и ранее, основная часть киберпреступлений совершаются с использованием сети Интернет — 300,3 тыс. (+91,3%) и средств мобильной связи — 218,7 тыс. (+88,3%). Каждое четвертое из них — кража или мошенничество (410,5 тыс.).

Второе. Киберапокалипсис

Технологическое вооружение киберпреступников к 2025 г. позволит им осуществлять ***целенаправленные атаки на предприятия с целью причинения физических повреждений и убийства людей***. Как прогнозируют специалисты исследовательской компании «Gartner», использование военизированных операционных технологий и других IT-систем только с учетом случаев смертельного исхода к 2023 г. нанесет ущерб по всему миру на сумму более 50 млрд долл.

Инциденты безопасности, связанные с операционными технологиями, эксперты разделяют на три основных класса по мотивации преступников: нанесение прямого физического ущерба; коммерческий вандализм, ведущий к нарушению производства; репутационный вандализм, в результате чего производитель признается ненадежным и не заслуживающим доверия.

Третье. Использование криптовалюты для отмывания денег

Основные цели отмывания денег заключаются в том, что киберпреступники, крадущие криптовалюту или принимающие ее в качестве оплаты незаконных товаров, должны скрыть источник своих средств и конвертировать криптовалюту в наличные, чтобы затем тратить их или хранить в банке. Благодаря усилиям правоохранительных органов киберпреступники не могут обменять свою незаконно полученную криптовалюту на фиатную и обналичить ее как обычный пользователь. Поэтому они полагаются на небольшую группу поставщиков услуг по отмыванию своих криптоактивов.

Правоохранительные органы могут создать существенные помехи киберпреступникам для конвертации криптовалюты в наличные, преследуя поставщиков услуг по отмыванию денег и тем самым сокращая стимулы для киберпреступников, в первую очередь использующих криптовалюту.

Исторически сложилось так, что ***основным направлением незаконной криптовалютной деятельности были крупные биржи, и это не изменилось в 2020 г.*** Фактически, доля всей незаконной криптовалюты, полученной биржами, в 2020 г. выросла.

Кроме того, значительный объем трафика перемещается с незаконных адресов на услуги, которые относятся к категории «рискованные», включая биржи с высоким риском, игровые платформы и сервисы со штаб-квартирами в юрисдикциях с высоким уровнем риска.

Четвертое. Квантовые вычисления

Полноценный квантовый компьютер — это дело будущего. Пока существуют лишь экспериментальные действующие ***макеты полноценных квантовых компьютеров***. Макеты в том смысле, что они работать уже могут, но ориентированы на строго определенные операции.

Однако анализ динамики развития квантовых вычислений позволяет с уверенностью утверждать, что мы имеем дело с так называемой экспоненциальной технологией. ***В 2019–2020 гг. произошел перелом. Если еще пару-тройку лет назад наиболее продвинутые, имеющие за плечами выдающиеся достижения специалисты в области IT полагали, что практическое применение квантовых компьютеров — дело конца 20-х — начала 30-х гг., то сегодня они с уверенностью утверждают о приходе эры квантовых компьютеров буквально в течение ближайших четырех-пяти лет.***

Всех беспокоит то, что кто-то, оказавшийся первым в этой гонке, сможет выбрать такой вариант: незаметно начать получать всю выгоду и не объявлять об этом всему миру.

Как любая технология новой промышленной революции квантовый компьютер несет для общества крупные выгоды и катастрофические угрозы. Он может преобразить банковское дело, может создать мощную систему киберзащиты, может на порядок усовершенствовать систему защиты от любого военного нападения, а ***может стать страшным оружием в руках террористов или мафиозных структур***.

Наиболее серьезные угрозы глобальной и национальной безопасности, экономике и повседневной жизни несет в себе использование квантовых компьютеров для взлома кодов. Специалисты по криптографии Агентства Национальной Безопасности США еще в 2015 г. опубликовали на сайте АНБ отчет, где выразили серьезную обеспокоенность перспективой появления работающих квантовых компьютеров, поскольку это может привести к чрезвычайно быстрой расшифровке многих использующихся сегодня криптографических алгоритмов. Представители АНБ отмечали, что вопрос разработки криптостойких алгоритмов, способных эффективно шифровать данные в эру квантовых компьютеров, актуален как никогда. По мнению специалистов Агентства, вполне реально появление работающего квантового компьютера, существование которого поставит под угрозу сохранность государственных и коммерческих данных во всех сферах. Хотя время от времени в ведущих мировых медиа появляются статьи об угрозах квантовых компьютеров для международных расчетных систем, процессинговых компаний типа *MasterCard*, *Visa* и т.п., а также криптовалют и в первую очередь биткоина, реальная ситуация благоприятнее, чем описываемые сценарии.

Дело в том, что ***к настоящему времени разработаны и через два-три года будут готовы для практического использования так называемые постквантовые методы криптографии***. Они базируются на сложнейшей математике, а их применение не позволяет квантовым компьютерам вскрывать корпоративные и федеральные сети, как консервный нож банку. Более того, ***во второй половине 2020 г. уже были проведены испытания прототипов квантовоустойчивой системы шифрования***, выстоявшей перед атакой квантового компьютера Google.

Главный недостаток систем постквантового шифрования — это не только чрезвычайно высокая цена их разработки, но и связанные с практической эксплуатацией огромные издержки на защиту данных, как хранящихся в базах данных, так и передаваемых от телекоммуникационных систем.

Самая большая угроза квантовых компьютеров мировой экономике и повседневной жизни состоит в следующем. ***Даже на начальной стадии квантовые компьютеры могут практически мгновенно сломать любой «антивирусник» и получить доступ, согласно мнению АНБ, примерно к 97% индивидуальных компьютеров, смартфонов и ноутбуков и не менее чем к 65% — корпоративных.*** Поскольку постквантовое шифрование не только на стадии разработки, но и на стадии эксплуатации требует больших

денег, оно, без сомнения, будет развернуто в ближайшие два-четыре года для федеральных органов власти, систем национальной безопасности и правопорядка, в ведущих научных центрах и крупнейших компаниях. Причем далеко не во всех странах, а только в некоторых. Среди них будут, безусловно, США, Китай, Япония, Южная Корея и Россия.

Что же касается всех персональных устройств, IT-инфраструктур малого и среднего бизнеса, они окажутся беззащитными против квантового компьютера в том случае, если он попадет в руки преступников, а тем более террористов или хакерских сетей. Это — мало осознаваемая, но абсолютно реальная угроза подрыва безопасности, угроза коммерции, а главное — повседневной жизни граждан.

Пятое. Цифровой след и его значение для оперативно-розыскной деятельности

В вышедшей в 2019 г. книге профессора Гарвардской школы бизнеса ***Шошаны Зубофф «Эра надзорного капитализма» («The Age of Surveillance Capitalism»)*** отмечается, что в последние десятилетия все большую силу набирает цифровой капитализм, который ассоциируется в первую очередь с *Google*, *Apple*, *Amazon*, *Microsoft* и *Facebook*. Воспользовавшись доверием пользователей, эти компании, анализируя большие массивы данных, следят за нами, проникая во все сферы жизни, как личной, так и общественной.

Они эксплуатируют человеческие стремления и эмоции, отслеживают наши вкусы, поведение, предпочтения с помощью алгоритмов. Доступ к этим данным могут получить все, кто пожелает, от производителей товаров до политических деятелей и, естественно, сотрудников полиции и спецслужб.

Шошана Зубофф назвала такую ситуацию ***капитализмом слежки***.

Что представляет собой, по ее мнению, надзорный (шпионящий) капитализм? Он жаждет заполучить человеческий опыт, ***все стороны человеческой жизни в качестве сырья для перевода в поведенческие данные***. Некоторые из них действительно используются для улучшения продукта или услуги, но ***все они используются в работе алгоритмов, которые превращают их в инструмент прогнозирования поведения***.

С помощью массива данных алгоритм может просчитать, что человек будет делать сейчас, вскоре и в более далеком будущем. Он составляет прогнозы поведения, которые очень востребованны на недавно образовавшемся рынке. Следящие за нами компании

новой формации чрезвычайно обогатились благодаря этим продажам, которые позволяют многим компаниям уверенно прогнозировать спрос на свою продукцию.

В качестве данных используется все, чем мы готовы поделиться в цифровом мире: наши мнения, предпочтения, события, эмоции, вкусы — все, что составляет нашу жизнь. И это еще не все: ***алгоритмы не только просчитывают наше поведение, но и умеют его формировать***. Таким образом, ***не мы управляем автоматизированными потоками, а они начинают управлять нами.***

В XXI в. на наших глазах формируется новая современность — ***слияние капитализма и цифровых технологий***. Существующие в мире законы о слежке ничего не могут сделать с защитой конфиденциальности.

Данные пользователей — это их собственность, но надзорный капитализм отбирает ее с помощью целого цикла действий.

Цикл включает четыре стадии: вторжение, формирование привыкания, адаптация и перенаправление.

На первом этапе происходит вторжение в незащищенное пространство: телефон, ноутбук, страницу в интернете, электронную почту, социальные сети, а вместе со всем этим — вторжение в ваши чувства и мысли.

Вторжение происходит до тех пор, пока не встретит сопротивление.

После окончания первого этапа наступает ***второй***: противник игнорируется, подавляется или соблазняется. Это происходит, когда против *Google* пытаются действовать общественные или антимонопольные организации. Компания может предложить доступ к данным, или эксклюзивной информации, или другие соблазны.

Протесты юристов и общества вызывают сбор личной информации с помощью Wi-Fi и камер *Street View*, контроль голосовой связи, пренебрежение к конфиденциальности, манипулирование поисковой системой, хранение пользовательских запросов, отслеживание геолокации смартфонов, камеры с распознаванием лиц и тому подобное во всех сервисах и устройствах *Google*.

Постепенно в обществе начинает развиваться привыкание к действиям *Google*, благо у людей перед глазами много примеров ухода компании от ответственности. Слишком многие заинтересованы в доступе к данным и потому оказывают негласную поддержку.

Люди начинают относиться к деятельности компании как к чему-то само собой разумеющемуся, смиряясь с неизбежным и находясь в растерянности. Пиратская деятельность цифровых гигантов становится частью реальности, и сторонникам конфиден-

циальности довольно трудно действовать в условиях нарастающего равнодушия общества.

На третьей стадии цикла руководители *Google* производят отвлекающие косметические изменения в своей работе, чтобы от них отстали проверяющие органы и не возмущалось общественное мнение.

На четвертой стадии они так перенаправляют сбор данных, что он кажется вполне законным. Но сбор и продажа данных никогда не останавливаются.

Надзорный капитализм принимает все новые формы.

Данные собирают не только интернет-гиганты, но и телекоммуникационные и кабельные компании, предоставляющие услуги людям и домохозяйствам. По сбору данных им не перегнать *Facebook* или *Google*, но они действуют в той же манере — полное пренебрежение к конфиденциальности.

Некоторые компании предоставляют услуги видеонаблюдения. Есть приложения, которые определяют кредитоспособность человека на основе его смартфона и поведения в интернете. Они анализируют тексты, написанные пользователем, электронную почту, GPS-координаты, сообщения в аккаунте *Facebook*, розничные покупки и пр.

Подобные приложения позволяют отслеживать частоту зарядки аккумулятора телефона, количество входящих сообщений, ответы на телефонные звонки, количество контактов в телефоне и расстояние, на которое перемещается владелец смартфона. ***Эти поведенческие данные превращаются в модели поведения, оценивающие кредитоспособность человека при помощи алгоритма, который благодаря накоплению и обновлению данных постоянно совершенствуется.***

Другие компании осуществляют глубокую проверку потенциальных сотрудников для работодателей или для арендодателей, если человек хочет снять жилье или офис. Арендодатель просит его предоставить доступ ко всем аккаунтам в социальных сетях. Затем ***специальная программа обрабатывает все содержимое аккаунта и выдает полный аналитический отчет о личности человека, финансовых возможностях, статусе, физическом состоянии, например о беременности.***

Сегодня интернет-гиганты, мобильные операторы и компании, специализирующиеся на «Интернете вещей», не только собирают данные пользователей, но и пытаются влиять на них. Они встраивают в страницы шпионские программы, выявляют с помощью алгоритмов наши привычки, улавливают наши эмоции, чтобы превра-

тить всю нашу жизнь в бесплатное сырье, которое потом с выгодой продадут.

Facebook многими воспринимается как убежище, место, где можно общаться с друзьями и единомышленниками, рассказывать о своей жизни, вкусах и предпочтениях. Но он устроен намного сложнее. Это ***огромный источник предсказательного поведенческого избытка***.

Все стороны личности, которые отражены в аккаунтах, можно преобразить в измеримое поведение. Машинный интеллект превращает эти данные в продукты прогнозирования. С такими возможностями можно адаптировать рекламу к личности пользователя и представлять информацию таким образом, чтобы человек был наиболее к ней восприимчив.

Пользователи *Facebook* в большинстве своем не знают, насколько уязвимыми они становятся, сообщая в социальной сети информацию о себе.

Facebook установил ***собственные социальные нормы***.

Один из способов воздействия — это настройка. Она способна включать подсознательные сигналы для формирования нужного поведения в нужном месте и в нужное время. Один из видов настройки — ***подталкивание***, когда поведение людей изменяется предсказуемым образом.

В сети используется цифровое подталкивание в коммерческих целях, которое незаметно воздействует на людей, навязывая им определенное поведение.

Путем подсознательного воздействия с использованием определенного эмоционального контента в сети можно заставить людей изменить свое поведение, реагируя на этот контент. Чем больше человек склонен к эмпатии, тем восприимчивее он к эффекту заражения эмоциями — об этом хорошо знают и психологи, и команда *Facebook*. Эмпатия ориентирует людей на других, заставляя разделять их переживания.

Вокруг использования цифровых следов человека ведется немало дискуссий правового и этического характера. Но кто бы как к этому ни относился, цифровые следы — это данность, которую нельзя не использовать в ОРД. И здесь тоже необходимы научные исследования.

Указанные направления использования ОРД являются определяющими на ближайшие годы. Но существует немало повседневных проблем цифровизации, требующих научного осмысления в рамках теории ОРД и практической реализации. Именно они

рассматриваются в настоящем сборнике в статьях специалистов в сфере теории ОРД.

Сборник посвящен памяти безвременно ушедших в 2020–2021 гг. выдающихся ученых — профессоров ***Константина Константиновича Горяинова, Валерия Михайловича Атмажитова*** и ***Валерия Павловича Кувалдина,*** внесших неоценимый вклад в развитие теории ОРД[1].

В.С. Овчинский

[1] Настоящее издание является логическим продолжением сборника «Актуальные проблемы теории оперативно-розыскной деятельности» (под общ. ред. К.К. Горяинова, В.С. Овчинского). М.: ИНФРА-М, 2017.

Раздел I
КИБЕРБЕЗОПАСНОСТЬ В СИСТЕМЕ ОПЕРАТИВНО-РОЗЫСКНОЙ, РАЗВЕДЫВАТЕЛЬНОЙ И КОНТРРАЗВЕДЫВАТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ

П.П. Городов

О транснациональном характере современной киберпреступности и задачах по противодействию ей со стороны субъектов оперативно-розыскной деятельности

Как эффективно бороться с современной киберпреступностью? Существует целый ***комплекс факторов***, которые в значительной мере осложняют проведение мер по противодействию ей.

Среди них — трансформация способов шифрования данных, максимально повышающих анонимность злоумышленников, отсутствие непосредственного контакта с потерпевшим, охват широкой аудитории, простота доступа к информации и, конечно же, ***трансграничный характер деяний, совершаемых в цифровой среде***.

С учетом указанных обстоятельств очевидно, что на национальном уровне с этим не справится ни один отдельно взятый государственный орган, как и на международном уровне — ни одно отдельно взятое государство.

Действовать и внутри страны, и за рубежом нужно сообща, единым фронтом. ***Функцию координации*** деятельности государственных органов в области противодействия информационной преступности в России выполняет Генеральная прокуратура Российской Федерации.

В июле 2020 г. этот вопрос обсуждался на Координационном совещании руководителей правоохранительных органов Российской Федерации под председательством Генерального прокурора РФ И.В. Краснова.

По итогам этого мероприятия был решен целый ряд организационных задач, выработаны согласованные с иными ведомствами меры, такие как:

— разработка единых критериев отнесения преступлений к совершенным с использованием информационно-коммуникационных технологий (ИКТ);

— проведение анализа положений национального законодательства в целях его совершенствования;

— планирование дополнительных проверочных мероприятий, например по пресечению фактов незаконной реализации сим-карт;

— определение проблем во взаимодействии следственных и оперативных подразделений субъектов ОРД.

Уже сейчас можно говорить о положительных примерах скоординированной нами работы.

Так, результатом осуществленного правоохранительными органами комплекса оперативно-розыскных мероприятий (ОРМ) и следственных действий, проведенных практически синхронно в 62 точках, расположенных в 11 субъектах Российской Федерации, стало задержание 30 активных членов и руководителей хакерской организованной преступной группы (ОПГ). В итоге ОПГ прекратила свое существование вместе с почти сотней интернет-магазинов, предназначенных для оборота запрещенных предметов.

Кроме того, ведется работа по активизации инструментов государственно-частного партнерства, поскольку ключевое значение для эффективного противодействия киберпреступлениям имеет качество взаимодействия с организациями, располагающими оперативно значимой информацией. Речь идет о банках, операторах связи, владельцах интернет-сервисов, центрах реагирования на компьютерные инциденты и об организациях сферы кибербезопасности.

Вместе с тем можно сколь угодно совершенствовать методы противодействия киберпреступности, но до тех пор, пока люди будут сообщать мошенникам свои платежные данные, хищения будут продолжаться.

Именно поэтому Генеральная прокуратура РФ активно участвует в процессах профилактики рассматриваемых преступлений, в том числе путем правового просвещения через официальный аккаунт в социальных сетях.

В то же время для принятия эффективных скоординированных мер проведения только одного координационного совещания недостаточно.

Именно поэтому было принято решение о создании под эгидой Генеральной прокуратуры РФ ***межведомственной рабочей группы по противодействию информационной преступности***.

Этот постоянно действующий орган образован в июле 2020 г. для решения оперативных задач в рассматриваемой сфере.

Помимо традиционных участников координационной деятельности — правоохранительных органов, группа также включает представителей МИДа России и Минюста России, поскольку в ее задачи входит не только проработка национальных вопросов, касающихся повышения эффективности работы правоохранительных органов в борьбе с киберпреступностью, но и ***выработка консо-***

лидированной российской позиции по этой теме на международной арене, в том числе в работе специального межправительственного комитета экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию ИКТ в преступных целях.

26 мая 2021 г. в Нью-Йорке в ходе заседания 75-й сессии Генеральной Ассамблеи ООН консенсусом принята ***российская резолюция 75/282 «О противодействии использованию информационных и коммуникационных технологий (ИКТ) в преступных целях».*** Документ определяет модальности работы специального комитета для разработки под эгидой ООН универсальной международной конвенции по борьбе с использованием ИКТ в преступных целях (спецкомитета), решение о создании которого было принято в 2019 г. по инициативе России при поддержке 46 государств.

Предусмотрено, что сессии спецкомитета пройдут поочередно в Нью-Йорке и Вене начиная с января 2022 г. Орган будет стремиться принимать решения консенсусом, однако предусмотрена возможность голосования, если консенсуса достигнуть не удастся. Проект конвенции должен быть представлен на рассмотрение 78-й сессии Генассамблеи ООН в 2023 г.

Консенсусное принятие российского проекта резолюции демонстрирует понимание международным сообществом серьезности угрозы информпреступности и необходимости выработки универсальных правил борьбы с ней. Запущен открытый, инклюзивный и транспарентный процесс переговоров по проблематике противодействия информпреступности под эгидой ООН.

Предложенный Россией подход фактически закрепляет ***цифровой суверенитет государств над своим информационным пространством*** и открывает новую страницу в истории глобального противодействия киберкриминалу. В практическом плане под эгидой Генассамблеи ООН создается переговорная площадка для разработки универсальной конвенции по борьбе с киберпреступностью. Таким международным органом станет спецкомитет, в который войдут эксперты из всех стран мира. В свое время аналогичный путь прошли Конвенция ООН против коррупции и Конвенция ООН против транснациональной организованной преступности.

Данная конвенция видится России и ее единомышленникам как очередной универсальный международный уголовно-правовой инструмент, сфокусированный на преступлениях в сфере использования ИКТ, направленный на борьбу с их противоправным применением и носящий по своему содержанию всеобъемлющий ха-

рактер. Конвенция должна основываться на принципах уважения государственного суверенитета и невмешательства во внутренние дела государств.

Положено начало субстантивной работе над конвенцией, которая будет учитывать интересы всех без исключения стран и основываться на принципах суверенного равенства сторон и невмешательства во внутренние дела государств. Процесс будет носить динамичный характер и будет завершен в 2023 г.

Для России как инициатора этого процесса консенсусный запуск работы спецкомитета — важный дипломатический успех, ***результат огромной работы российского МИДа***.

Подготовленный проект конвенции имеет целый ряд преимуществ. Он учитывает современные вызовы и угрозы в сфере международной информационной безопасности (в том числе криминальное использование криптовалюты), вводит новые составы преступлений, совершаемых с использованием ИКТ (распространение фальсифицированной медицинской продукции, оборот наркотиков, вовлечение несовершеннолетних в совершение противоправных деяний, опасных для их жизни и здоровья, и др.). Кроме того, проект расширяет сферу международного сотрудничества в вопросах выдачи и оказания правовой помощи по уголовным делам, включая выявление, арест, конфискацию и возврат активов.

27 июля 2021 г. в штаб-квартире ООН в Вене межведомственная российская делегация, возглавляемая заместителем Генерального прокурора Российской Федерации, на встрече с и.о. исполнительного директора Управления ООН по наркотикам и преступности Деннисом Чатчавалитом официально внесла российский проект конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также передала копию проекта конвенции председателю специального комитета ООН по разработке конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях Фаузие Мебарки.

Какие вопросы, важные для следственных и оперативных подразделений, в первую очередь будут обсуждаться в работе по проекту конвенции? Например, следующие.

Какая информация предоставляется в инициативном порядке? Может ли государство-участник в пределах норм своего внутреннего законодательства направить без предварительного запроса другого государства-участника информацию, полученную в рамках своего собственного расследования, когда, по его мнению, раскрытие такой информации могло бы помочь другому государству-

участнику начать или провести расследование? Каковы должны быть условия конфиденциальности работы с информацией?

Как будет осуществляться защита персональных данных? Какие персональные данные могут быть использованы и для каких целей?

Как будут проводиться процедуры направления запросов о взаимной помощи в отсутствие применимых международных соглашений?

Как будут проводиться допросы и иные процессуальные действия с использованием систем видео-конференц-связи или телефонной конференции?

Каковы условия выдачи преступников?

Как будет оперативно обеспечиваться сохранность информации в электронной форме? Какие сведения, идентифицирующие владельца информации или местоположение устройства ИКТ, необходимы?

В каких случаях в исполнении запроса об обеспечении сохранности информации может быть отказано? Например, если запрашиваемое государство-участник полагает, что исполнение такого запроса может нанести ущерб его суверенитету, безопасности или другим существенным интересам.

Как будет осуществляться оперативное предоставление сохраненных технических параметров трафика?

Как будет осуществляться взаимная помощь в отношении доступа к хранящимся электронным данным?

Может ли государство-участник попросить другое государство-участника произвести обыск или аналогичные обеспечивающие доступ действия, выемку или аналогичное обеспечение сохранности и раскрытие данных, хранящихся с помощью компьютерной системы, которая находится на территории запрашиваемого государства-участника?

Как будет осуществляться взаимная помощь по сбору технических параметров трафика в режиме реального времени?

Каким путем могут создаваться органы по проведению совместных расследований?

Каким образом могут реализовываться специальные методы расследования, такие как электронное наблюдение или другие формы наблюдения и агентурные операции, на своей территории, чтобы доказательства, собранные с помощью таких методов, допускались в суде?

Как будет осуществляться обмен в надлежащих случаях с другими государствами-участниками информацией о конкретных средствах и методах, применяемых для совершения преступлений,

охватываемых указанной конвенцией, включая образцы вредоносного программного обеспечения, использование поддельных удостоверений личности, фальшивых, измененных или поддельных документов и других средств для сокрытия противоправной деятельности? Как для этих целей будет использована Международная организации уголовной полиции — Интерпол?

Каковы будут меры по возвращению имущества, формы предупреждения и выявления переводов доходов от преступлений, в том числе связанных с оборотом цифровых финансовых активов и цифровой валюты?

* * *

В то же время понятно, что это процесс небыстрый. Согласование текста глобальной конвенции и ее открытие для подписания займут не один год.

Поэтому Генеральная прокуратура Российской Федерации параллельно движется по пути ***укрепления двусторонней базы сотрудничества***.

Прежде всего речь идет о межправительственных соглашениях, работа над которыми ведется МИДом России.

Кроме того, федеральным законом Генеральная прокуратура наделена полномочиями по осуществлению прямых связей с компетентными органами других государств и международными организациями, в том числе по заключению с ними межведомственных соглашений и иных договоренностей.

Этими полномочиями мы активно пользуемся. К настоящему времени у нас насчитывается более 90 соглашений с иностранными партнерами. За последний год заключено четыре из них: с генеральными прокуратурами Бразилии, Португалии, Белиза и Армении. При этом в каждом из четырех соглашений вопросы взаимодействия в области противодействия киберпреступлениям поставлены во главу угла. Эти вопросы мы также включаем в программы сотрудничества с министерствами юстиции и прокуратурами зарубежных государств, разрабатываемые на краткосрочный период — обычно два-три года.

Кроме того, в декабре 2020 г. тема противодействия киберпреступности стала ключевой на встрече руководителей прокурорских служб стран БРИКС, проведенной под председательством России. Подписан итоговый документ, определивший рамки международного взаимодействия.

С.К. Кузнецов

Кибервойна с кибермошенниками: антифрод Сбербанка России и взаимодействие с оперативными подразделениями МВД России и ФСИН России

Еще несколько лет назад преступления в сфере ИКТ не имели такого масштаба, способного навредить большому количеству людей. Основными инструментами оперативных работников полиции были блокнот и ручка. В сегодняшнем цифровом мире вчерашние условия работы недопустимы.

Глобальные ИТ-тренды и киберугрозы вынуждают работать совершенно иначе. Мировое сообщество признает, что кибератаки — это один из глобальных рисков, угрожающих человечеству сегодня. Об этом предупреждают эксперты Всемирного экономического форума, которые ежегодно публикуют доклад о глобальных рисках. Аналитики уверены, что *киберпреступность и мошенничество в интернете так же опасны, как экологические катастрофы и необратимые климатические изменения*. Всего за несколько лет мошенники проделали путь от примитивных схем обмана типа скимминга или заражения устройств вирусами до «взлома» человека с помощью методов социальной инженерии.

По итогам 2020 г. Россия заняла первое место в мире по совокупному количеству различных кибератак, направленных на жителей страны, включая банковские зловреды, вирусы-шифровальщики, программы-майнеры, IoT-угрозы, атаки через веб-ресурсы. Этот результат отражен в исследовании «Лаборатории Касперского» (*Kaspersky Security Bulletin 2020*), подготовленном на основе данных миллионов пользователей по всему миру.

По данным ЦБ РФ, число атак на клиентов банков с использованием методов социальной инженерии в 2020 г. выросло почти в 2 раза (на 88%) по сравнению с 2019 г. В подавляющем большинстве случаев (84%) мошенники связываются со своими жертвами по телефону.

В 2012 г. основную массу преступлений в *Сбербанке* составлял скимминг. В 2017 г. нам удалось побороть эту проблему благодаря изменениям законодательства и внедрению технических мер.

К 2020 г. мы практически уничтожили вирусные атаки на клиентов Сбербанка.

Киберпреступники знают, что средства на счетах банка надежно защищены, поэтому предпочитают атаковать клиентов. Сейчас более 90% всего мошенничества осуществляется с помощью приемов социальной инженерии. Телефонное мошенничество в России приобрело масштабы национального бедствия. Банки находятся на острие проблемы, потому что первыми фиксируют мошеннические атаки и видят проблемы клиентов. 15 млн — это количество мошеннических звонков гражданам России, до 100 тыс. звонков в сутки. Около 3,7 млн жалоб клиентов на попытки телефонного мошенничества поступило в Сбер только в 2020 г. За четыре года число случаев телефонного мошенничества выросло более чем в 30 раз, по сравнению с 2019 г. мы видим двукратное увеличение.

Технологии развиваются стремительно, еще 10 лет назад не существовало IoT-устройств (видеокамеры, умные помощники, умные пылесосы), а сегодня с этих устройств происходят мощнейшие атаки — DDoS на организации. Например, в прошлом году Сбербанк успешно отразил мощную DDoS-атаку, которую совершили 15 тыс. подключенных к интернету видеокамер.

Технологические возможности (в том числе для киберпреступников) становятся все шире. Если сейчас мы боремся с телефонным мошенничеством и фишингом, то через несколько лет нам предстоит решать куда более трудные задачи: например, противостоять атакам на устройства, оснащенные искусственным интеллектом, или распознавать кражу личности с помощью технологии DeepFake.

Против клиентов действуют многочисленные *криминальные «кол-центры»* (часть из которых проникли даже в учреждения ФСИН России). Они в среднем «зарабатывают» миллион долларов в месяц. Причем многие из этих «кол-центров» орудуют на территории ближнего зарубежья. В половине случаев абонент снимает трубку. 70% отказываются от разговора, а с остальными 30% мошенники начинают работу. Доход среднестатистического криминального «кол-центра» составляет 65 млн руб. в месяц. 20 — человек в смене. 6000 долл. США — зарплата смотрящего. 7000 звонков в сутки. Зарплата одного «специалиста» в неделю — от 700 до 250 тыс. руб. Преступники используют сервисы IP-телефонии, которые позволяют им звонить гражданам с подстановкой любого номера. Таким образом осуществляется более 90% мошеннических звонков. Мошенниками используются легальные операторы, предоставляющие услуги виртуальной АТС. Стоимость — 1000 руб.

в месяц. В пакет входит аренда номера 495/499 плюс полноценная CRM-система. Простая регистрация на сервисе — логин плюс пароль.

Сами кибермошенники очень быстро реагируют на новостную повестку. Возникают новые информационные поводы, которые мошенники тут же начинают использовать в своих целях. Примером может послужить стремительный рост популярности социальной сети *Clubhouse*, который привел к появлению новых видов мошенничества: продажа фейковых приглашений в соцсети, создание поддельных приложений.

Идентификация и аутентификация — краеугольный камень построения инфраструктуры цифрового государства. Специфические угрозы для идентификации — синтетические личности, дипфейки. Биометрическая идентификация позволяет кардинальным образом изменить клиентский опыт, повысить удобство пользования всевозможными услугами, в том числе банковскими. При этом любая технология сопряжена с рисками кибербезопасности. В условиях стремительного развития технологий ИИ (синтез изображений и речи) повышаются риски успешных атак на системы, использующие биометрию. Поэтому для критичных операций или услуг биометрия используется в банке в качестве одного из факторов аутентификации, не является единственным фактором.

К середине 2020 г. как минимум шесть стран проводили *эксперименты с цифровой национальной валютой*, в том числе Китай, Южная Корея, Швеция, начавшая эту работу одной из первых. В начале октября о возможном выпуске национальной цифровой валюты и начале экспериментов с цифровым евро объявил Европейский ЦБ, эмитент второй по значимости валюты в мире. Преступники внимательно следят за развитием цифровых валют и уже оттачивают свое мастерство на примере биткоинов. Например, в конце 2020 г. биржа криптовалют EXMO подверглась кибератаке и лишилась около 5% всех активов, хранившихся в «горячих» кошельках (52 млн долл.).

Квантовый компьютер — угроза традиционной криптографии. Квантовый компьютер уничтожит большинство традиционных алгоритмов (RSA, DSA, ECDSA).

ИИ для кибератак и для защиты. Технологии ИИ могут использоваться киберзащитниками для выявления атак и нейтрализации угроз. Однако, оказавшись в руках злоумышленников, технологии станут опасным оружием и будут представлять серьезную угрозу. ИИ открывает большие возможности для киберзлоумышленников,

позволяя им увеличивать силу атак в плане скорости, объема и сложности до огромных масштабов.

Со временем «обогащенное» ИИ вредоносное ПО научится самостоятельно распространяться, выискивая любые возможные уязвимости для компрометации сети. «Представьте себе атаку червя типа WannaCry, который бы вместо выбора одной формы бокового смещения (например, эксплойта EternalBlue) самостоятельно определял целевую среду и соответственно выбирал методы проникновения. Например, ИИ-программа может «понять», что ее нацелили на уже исправленные уязвимости, и провести атаку методом подбора еще неисправленных, которая задействует кейлогинг и другие методы, доказавшие свою эффективность при проведении целевых атак. Особую опасность ИИ-зловредам придает тот факт, что они могут сидеть в засаде, учиться, подбирать техники атаки, но делать все это без участия серверов команд и управления.

ИИ может обеспечить канал не только для крайне быстрых, но и маломощных и медленных (*low and slow*) атак. Уже известен такой случай с компанией, которая занимается медицинскими технологиями. Особенность ситуации заключается в том, что ее данные уводились хакерами на продолжении длительного времени и столь крошечными пакетами, что они не превышали пороговых значений объема данных, допускаемых инструментами безопасности. Анализ вторжения показал, что множественные подключения к сети компании осуществлялись с внешнего IP-адреса. При этом передаваемый пакет данных на каждый канал не превышал 1 Мб. Таким образом, хакерам за относительно короткое время удалось похитить 15 Гб информации. Злоумышленники сумели украсть имена пациентов, адреса и истории болезни.

Работа антифрод-системы Сбера

Для выявления разного рода мошенничества в Сбербанке применяется уникальная система фрод-мониторинга. Система построена на основе алгоритмов ИИ, применяются собственная графовая база данных и графовая аналитика.

Все существующие каналы взаимодействия клиента и банка подключены к ***Антифроду*** (программный комплекс для борьбы с мошенничеством). Это позволяет Сбербанку легко выявлять кросс-канальные атаки на клиентов.

В режиме реального времени в течение 100 мс система выдает вердикты на основе тысяч параметров по каждой транзакции, которых происходит около 380 млн в сутки.

Кроме анализа транзакций система анализирует рисковые события от телекомов, действия сотрудников, операции в автоматизированных системах, нефинансовые операции — по факту это система управления цифровыми рисками организации. В месяц анализируется 10 млрд нефинансовых операций.

Сбер активно внедряет *технологии ИИ при борьбе с мошенничеством*. ИИ-модели Сбера эффективно выявляют связи между клиентами, кластеризуют мошеннические группы, выявляют нетипичные геолокационные паттерны перемещений, аномальные скорости передвижений и пр. То, что еще вчера казалось невозможным и фантастическим, — сегодня уже реальность. Антифрод-система Сбербанка уже научилась останавливать 99% всего телефонного мошенничества.

Эффективность работы этой системы обусловлена тесным сотрудничеством с операторами связи, также отслеживающими подозрительные звонки, что позволяет оперативно реагировать на возникающие угрозы.

ИИ-модели — один из модулей системы — разработанная банком real-time-среда исполнения моделей. Эта среда позволяет внедрять в процесс оценки ИИ-модели собственной разработки. Сейчас в системе работают свыше 15 ИИ-моделей, оценивающих различные аспекты риска проведения операций.

BigData. Для максимальной эффективности работы Антифрода и AI-моделей система интегрирована с хранилищем больших данных. Это позволяет при принятии решений использовать всю доступную информацию о взаимодействии клиентов и банка (петабайты информации).

Антифрод позволяет Банку оперативно реагировать на новые возникающие вызовы, выводить новые продукты на рынок с сохранением максимального уровня защищенности его клиентов от мошенников.

Антифрод помогает также правоохранительным органам находить без вести пропавших людей (за квартал в среднем находят 250 человек).

Сбер внутри своей команды сделал анализ даркнета, и обнаружилось, что сегодня там огромное поле деятельности, где кибермошенники чувствуют себя достаточно свободно. Аналитики Сбера обнаружили не менее 33 соответствующих площадок и 2,33 млн так называемых аккаунтов. Это означает, что в данном обмене информацией могут участвовать около 2 млн человек.

Завтра технологии станут еще более доступными, и злоумышленники с любым уровнем квалификации и ресурсов смогут ими воспользоваться. Под угрозой информационная повестка, доверие к СМИ в целом. У злоумышленников появится возможность:

- влиять на биржевые котировки путем публикации ложных заявлений от имени публичных лиц компаний-эмитентов;
- влиять на деятельность компаний, выдавая себя за менеджмент в видеоконференциях с сотрудниками;
- влиять на репутацию граждан и должностных лиц;
- влиять на информационную повестку в стране и политические настроения.

Сбербанк в Лаборатории кибербезопасности также ведет исследование, и уже есть первый прототип, показывающий хорошие результаты для нескольких технологий создания DeepFake.

Алгоритм действий для кибероперативников

Можно создать отлаженную систему кибербезопасности в компании. Но без активного взаимодействия с оперативными подразделениями МВД России и ФСИН России необходимого эффекта в борьбе с киберпреступностью не будет, особенно в ОРМ по *ликвидации криминальных кол-центров*.

Для того чтобы успешно раскрывать киберпреступления, полицейский — оперативник завтрашнего дня должен не просто обладать опытом раскрытия преступлений, он должен быть *специалистом по кибербезопасности*. Но нельзя быть спецом по кибербезопасности без глубоких экспертных знаний в ИТ. Для расследования киберпреступлений ему придется использовать аналитические возможности Big Data, инструменты дополненной реальности, разбираться в сетевых протоколах взаимодействия устройств, хорошо понимать, как устроен цифровой мир.

Ключевой момент в эффективной борьбе с киберпреступностью — формирование у современных кибероперативников широкого набора знаний и навыков в различных областях: от банковских технологий (например, технологии обеспечения бесконтактных платежей, принципы работы эквайрингового оборудования) до глубоких знаний в ИТ-технологиях и технологиях кибербезопасности.

Огромную роль в этом должны сыграть вузы, которые готовят будущих сотрудников правоохранительных органов. Уже сегодня необходимо задуматься о расширении учебной программы и введении дисциплин, которые повысят уровень подготовки российских специалистов по противодействию киберпреступности.

Важно знакомить будущих сотрудников правоохранительных органов с технологиями ИИ, DeepFake и методами защиты от связанных с ними угроз, чтобы они могли поддерживать правопорядок в будущем в условиях новой цифровой реальности.

Ю.Н. Жданов, В.С. Овчинский

Кибермафия как объект оперативно-розыскного воздействия

Американская компания по киберзащите ***Cybersecurity Ventures*** ожидает, что глобальные затраты на киберпреступность будут расти на 15% в год и достигнут ***10,5 трлн долл.*** США в год к 2025 г. по сравнению с 3 трлн долл. США в 2015 г.

Риск киберпреступности для стимулов к инновациям и инвестициям экспоненциально больше, чем годовой ущерб, нанесенный стихийными бедствиями, и в криминальном плане выгоднее, чем мировая торговля всеми основными незаконными наркотиками в совокупности.

Приведенные цифры касаются только видимой части сети. Помимо нее в «теневом интернете» ущерб от киберпреступности вообще не поддается количественной оценке. По некоторым данным, размер теневой сети (которая не индексируется и недоступна для поисковых систем) в 5 тыс. раз превышает размеры официального интернета.

Темная сеть также является местом, где киберпреступники покупают и продают вредоносное ПО, наборы эксплойтов и системы кибератак, которые они используют для нанесения ударов по жертвам, включая предприятия, правительства, коммунальные службы и поставщиков основных услуг.

Организованные криминальные структуры, занимающиеся киберпреступностью, объединяют усилия, и вероятность их обнаружения и судебного преследования, согласно ***Отчету о глобальных рисках Всемирного экономического форума за 2020 год***, оценивается в 0,05%.

Европол в докладе об оценке угроз серьезной (тяжкой) и организованной преступности (апрель 2021 г.) досконально исследовал тенденции кибермафии.

Использование технологий — одна из главных особенностей тяжкой и организованной преступности в 2021 г. Преступники используют зашифрованную связь для контактов друг с другом, социальные сети и сервисы мгновенных сообщений для связи с более широкой аудиторией с целью рекламы нелегальных товаров или распространения дезинформации. Интернет и электронная ком-

мерция дают правонарушителям возможность получать доступ к знаниям и сложному современному инструментарию, облегчая совершение преступлений.

Социальные сети и системы мгновенного обмена сообщениями используются также для распространения дезинформации. ***Хотя распространение дезинформации само по себе часто не является преступным поведением, оно может поощрять преступную деятельность или содействовать ее осуществлению.*** Мошенники и фальсификаторы инициировали подобные кампании по распространению дезинформации в контексте пандемии COVID-19 для увеличения продаж своей продукции или для вовлечения жертв в мошеннические схемы.

Услуги киберпреступников можно приобрести, заплатив гонорар, абонентскую плату или процент от незаконной прибыли. В интернете, особенно в даркнете, широко предлагаются соответствующие криминальные инструменты, например вредоносное ПО, программы-вымогатели, средства поддержки фишинга, анализаторы трафика, устройства для кражи данных с кредитных карт и распределенные атаки типа «отказ в обслуживании» (DDoS). Кроме того, продаются зашифрованные данные кредитных карт лиц, ставших жертвами мошенничества.

Модель «преступление как услуга» делает криминальные услуги легкодоступными для любого желающего, снижая уровень знаний и умений, который ранее требовался для совершения конкретных преступных действий. Наконец, интернет-платформы предоставляют инструкции по совершению большинства преступлений. Темы предлагаемых «руководств» и «учебных пособий» варьируются от производства синтетических наркотиков, изготовления примитивного огнестрельного оружия и самодельных взрывных устройств до всех видов киберпреступности.

Криптовалюты остаются важным средством оплаты нелегальных товаров и услуг. Децентрализация и полуанонимность обусловливают их привлекательность для осуществления преступных сделок. Мошенники особенно часто используют криптовалюты. Нелегальные доходы могут изначально иметь форму виртуальной валюты или могут быть конвертированы в цифровую форму. Новые методы отмывания денег с использованием криптовалют включают использование сервисов микширования и обмена монет.

Сегодня в интернете криминальный контент доминирует в таких областях, как торговля, коммуникация и доступ к информации. Цифровая трансформация экономики, общества

и частной жизни быстро прогрессирует и продолжит влиять на все аспекты жизни и деятельности человека. Неудивительно, что эти изменения оказали существенное влияние и на сферу тяжких преступлений и организованной преступности в ЕС. ***Практически все виды преступной деятельности теперь включают в себя онлайн-составляющие***, такие как цифровые решения, облегчающие коммуникацию для преступников.

Интернет-пространство изменило розничную торговлю и коммерцию. Цифровые торговые площадки сделали товары более доступными. Количество специализированных веб-сайтов и специализированных приложений быстро увеличилось, и они упростили доступ ко всем типам товаров и услуг. ***Трансформация легальной торговли нашла свое отражение и в криминальной сфере. Большинство противоправных действий были перенесены в интернет.*** Преступники используют и легальный, и теневой интернет, где они предлагают все виды запрещенных товаров и большинство нелегальных услуг. Наличие и доступность безопасных онлайн-каналов привели к диверсификации платформ, используемых для незаконной торговли в интернете. Распространение каналов связи с шифрованием данных и социальных сетей позволяет преступникам легко расширить аудиторию своих потенциальных клиентов.

Преступники используют различные контрмеры для обеспечения безопасности своих операций в сети Интернет и полагаются при этом на такие сервисы, как виртуальные частные сети (VPN), прокси-серверы и анонимные браузеры или «луковые» маршрутизаторы (TOR). Широко используются торговые площадки в социальных сетях, закрытые группы и мессенджеры, а также сервисы обмена зашифрованными сообщениями. Розничная торговля в интернете обеспечивает прямой доступ к более широкому кругу потребителей. Это привело к резкому росту использования небольших посылок, отправляемых через почтовые или курьерские службы, для распространения запрещенных и нелегальных товаров. Из-за большого объема почтовых отправлений снижается вероятность обнаружения небольших партий товара.

Социальные сети дублируют рекламу на веб-сайтах и служат выделенными каналами для маркетинга или каналами связи для криминальных сетей.

Некоторые провайдеры предлагают ***услуги безопасной связи с использованием модифицированных мобильных устройств***. У Европола есть предположения, что некоторые из этих услуг напрямую и преднамеренно обслуживают коммуникационные потребности преступников. Устройства, предлагаемые такими про-

вайдерами, якобы гарантируют полную анонимность и не имеют таких функций, как камера, микрофон, GPS, порты USB. Эти услуги устраняют любую связь между устройством или SIM-картой и пользователем. Зашифрованный интерфейс обычно скрыт и работает как часть двойной операционной системы. Подобные телефоны продаются через сети подпольных перекупщиков, а не через обычные точки розничных продаж.

Технологии шифрования широко используются как в законных, так и в незаконных целях. Шифрование обеспечивает конфиденциальность и целостность информации и защищает личные данные в процессе коммуникации. Сквозное шифрование стало стандартной функцией безопасности для многих каналов связи, включая приложения для обмена сообщениями и другие онлайн-платформы. Шифрование выгодно всем пользователям. К сожалению, это справедливо и в отношении преступников и криминальных сетей. Преступники уже много лет используют различные типы шифрования для защиты своих сообщений, передаваемых как через интернет, так и традиционными способами, от контроля со стороны правоохранительных органов.

Киберпреступность ежегодно приводит ***к значительным финансовым потерям для предприятий, частных лиц и государственного сектора из-за выплат разработчикам программ-вымогателей***, затрат на устранение последствий атак и расходов на усиление мер кибербезопасности.

Значительную угрозу представляют ***кибератаки, направленные на жизненно важные объекты инфраструктуры*** — они могут повлечь за собой серьезные последствия, включая гибель людей. Быстро набирающая темп цифровизация общества и экономики постоянно создает новые возможности для злоумышленников, причастных к совершению киберпреступлений. Постоянный рост числа пользователей сети Интернет ведет к появлению новых слабых и уязвимых сторон и увеличивает число потенциальных целей для кибератак.

Пандемия COVID-19 привела к резкому увеличению количества пользователей интернета как в частных, так и в корпоративных системах в 2020 г., поскольку удаленная работа стала нормой во многих секторах и отраслях. Это событие сделало многие корпоративные сети более уязвимыми для кибератак.

К киберпреступлениям относятся создание и распространение вредоносных программ, несанкционированный доступ к информационным ресурсам с целью кражи конфиденциальных личных или корпоративных данных, атаки типа «отказ в обслуживании»

(DDoS) с целью причинения финансового и (или) репутационного ущерба и другие преступные действия.

За последние годы возросло количество зарегистрированных кибератак, которые к тому же стали более изощренными. ***Статистика киберпреступлений, вероятно, в значительной степени занижена.***

Если ***ИИ*** используется в системах принятия решений, то манипулирование данными может иметь серьезные последствия для отдельных пользователей. Ожидается, что в будущем использование ИИ в преступных целях, включая использование ***технологии deepfake***, возрастет.

Вредоносное ПО — это распространенный тип кибератак, при котором вредоносный код проникает в компьютер, сеть или мобильное устройство, устанавливая контроль над системой. Цель атак с применением вредоносного ПО заключается в хищении данных (в том числе персональной информации), нарушении работы служб и шпионаже. Все чаще объектами кибератак становятся коммерческие предприятия. Государственные учреждения, включая жизненно важные секторы инфраструктуры, такие как службы здравоохранения, также являются мишенями для киберпреступников. Потенциальные утечки данных или сбои в работе служб в этих секторах могут нанести огромный финансовый и социальный ущерб.

Киберпреступники, осуществляющие атаки с помощью вредоносного ПО, в первую очередь стремятся к получению прибыли и в меньшей степени — к завоеванию репутации в хакерском сообществе. Вредоносное программное обеспечение — широко используемый киберпреступниками инструмент. Хакерские программы постоянно совершенствуются и отличаются большим разнообразием — количество вариантов измеряется сотнями тысяч. ***Агентство ЕС по кибербезопасности (ENISA)*** каждый день сообщает об обнаружении 230 тыс. новых штаммов вредоносных программ.

В ближайшие годы угроза киберпреступности, скорее всего, будет расти. Это касается как числа, так и технической сложности киберпреступлений. Киберпреступность отличается высокой динамичностью, поскольку использует быстроразвивающиеся технологии. Жизненно важные инфраструктуры по-прежнему будут служить мишенями для кибератак, и это представляет значительную опасность. Появление «Интернета вещей» (IoT), расширение сферы использования ИИ, распространение приложений, работающих с биометрическими данными, рост популярности ав-

тономных транспортных средств — все это окажет значительное влияние на мир. Эти инновации создадут и новые возможности для криминала.

Растление несовершеннолетних с использованием сети Интернет включает в себя все виды сексуальной эксплуатации, совершаемой в отношении ребенка, которые на каком-либо этапе связаны с онлайн-средой. Растление несовершеннолетних травмирует их и часто наносит серьезный ущерб физическому и психологическому благополучию жертв, что может привести к самоубийствам.

Этот тип эксплуатации, как правило, включает домогательства, систематические надругательства и словесное, психологическое и физическое насилие в отношении детей. В последние годы наблюдается неуклонное расширение деятельности, связанной с растлением несовершеннолетних с использованием сети Интернет. Сексуальная эксплуатация детей затрагивает наиболее уязвимых членов общества. К материалам, связанным с растлением несовершеннолетних, можно легко получить доступ на всех типах устройств, включая мобильные. Широко распространенное злоупотребление инструментами шифрования, включая приложения со сквозным шифрованием, снизило риск обнаружения злоумышленников.

Преступники все чаще полагаются на сервисы анонимизации, такие как виртуальные частные сети (VPN) или прокси-серверы. В последние годы неуклонно растет число зарегистрированных инцидентов, связанных с растлением несовершеннолетних посредством видеосвязи в режиме реального времени. Эта тенденция усилилась во время пандемии COVID-19. В результате введения для предотвращения распространения пандемии мер изоляции дети больше времени проводят в интернете без присмотра, что делает их более уязвимыми для злоумышленников. Хотя большинство случаев приходится на страны Юго-Восточной Азии (в первую очередь, на Филиппины), подобные правонарушения в последнее время были также зарегистрированы и в ЕС.

Материалы, связанные с растлением детей, обычно производятся в месте проживания жертвы лицами, входящими в круг доверенных лиц ребенка. Преступники используют вымышленные имена и специальные методы убеждения, чтобы завоевать доверие жертвы и получить нелегальный контент при помощи манипулирования или шантажа. Жертв часто записывают во время полового контакта, при этом они не подозревают о ведущейся видеосъемке. Преступники используют слово ***«кэппинг»*** (которое происходит от словосочетания «снимать материалы с участием жертв»), когда говорят о материалах такого рода. Записи, связанные с растле-

нием несовершеннолетних, обычно защищены паролем и хранятся на локальных устройствах или в онлайн-хранилищах. Компании, предоставляющие услуги хранения информации, часто не знают о материалах, размещенных на их серверах. Для хранения и распространения записей, содержащих сцены сексуальной эксплуатации детей, все чаще используются мобильные устройства. Дети сейчас нередко имеют неконтролируемый доступ к интернету. Это подвергает их риску растления со стороны преступников, поскольку они часто не обладают достаточным опытом, чтобы отличить дружеское отношение от злого умысла.

«Нормализация» сексуального поведения в интернете снижает порог для распространения собственноручно произведенного контента — по согласию или посредством принуждения. ***Увеличился объем материалов, производимых самими жертвами в результате манипуляций или шантажа.*** Растление несовершеннолетних на расстоянии в режиме реального времени относится к случаям, когда злоумышленник платит за трансляцию акта растления в прямом эфире через специальные платформы для распространения видеоконтента. Иногда акт растления снимают или записывают для дальнейшего распространения в интернете, что приводит к повторной виктимизации жертвы, как и в случае с другими видами материалов, связанных с растлением детей. В подавляющем большинстве случаев в ходе подобных прямых трансляций показывают девочек в возрасте младше 13 лет в домашней обстановке.

Европол в настоящее время располагает более чем 40 млн изображений, иллюстрирующих сексуальную эксплуатацию несовершеннолетних в разных странах мира.

Переход к безналичной экономике создает мощные стимулы для ***мошенников, специализирующихся на платежах***. Киберпреступники стремятся взломать системы онлайн-платежей, интернет-банкинга и мобильного банкинга, онлайн-заявки на осуществление платежей, сервисы бесконтактной оплаты (как с использованием кредитной карты, так и без нее) и мобильные приложения. Рост использования мобильных устройств для осуществления финансовых операций и процедуры аутентификации сделал их мишенью для киберпреступников.

Мошенничество с безналичными платежами включает в себя все виды мошеннических действий, связанных с наиболее распространенными методами оплаты, в том числе платежи с использованием и без использования кредитной карты. Кибермошенничество — это широкий спектр мошеннических схем, которые осуще-

ствляются исключительно или преимущественно в интернете. Они могут включать, в числе прочего:

— компрометацию корпоративной электронной почты. Целью данного вида мошенничества являются предприятия и организации. Количество и степень изощренности попыток преступников продолжают расти;

— новые методы совершения преступлений, такие как подмена SIM-карт.

Киберпреступники устанавливают контроль за использованием телефонного номера жертвы, по сути, дезактивируя SIM-карту жертвы и перенося номер на SIM-карту, принадлежащую члену преступной сети. Как правило, преступники осуществляют подмену от имени поставщика телефонных услуг: либо через сотрудника компании, являющегося на самом деле коррумпированным инсайдером, либо с помощью методов социальной психологии.

Телефонные операторы, используя выдуманные истории или сценарии, убеждают жертв совершить платеж, перевести деньги или осуществить авансовую оплату.

Намеренная имитация другого человека с целью обмануть кого-то, притворившись другим (полицейским, членом семьи) и чем-нибудь угрожая. Растет число мошеннических попыток получить конфиденциальную информацию или данные, например имена пользователей, пароли и реквизиты банковских карт, путем выдачи себя в электронной переписке за заслуживающее доверие лицо.

Мошеннические схемы с инвестициями наносят частным лицам и компаниям значительный финансовый ущерб. Такие мошенники все чаще нацеливаются на рынок инвестиций в криптовалюты, создавая фейковые сайты, предлагающие фиктивные инвестиционные возможности. Жертв мошенники, как правило, ищут в социальных сетях.

Аферы с социальными пособиями наносят существенный финансовый ущерб бюджету государств-членов и могут лишить государственной поддержки тех, кто действительно нуждается в помощи. Мошенничество с социальными пособиями включает в себя аферы с медицинской страховкой, социальным пакетом, пособиями по безработице или пособиями низкооплачиваемым рабочим и беженцам. В рамках мошенничества с социальным демпингом криминальные структуры создают фиктивные компании, запрашивая выплаты социальных пособий несуществующим сотрудникам. В рамках другой разновидности такого мошенничества сотрудники

продолжают работать, получая и пособие по безработице, и заработную плату по штатному расписанию работодателя.

Самой распространенной разновидностью банковского мошенничества является ***кредитное и ипотечное мошенничество***. Мошенники используют компании для получения ипотечных кредитов с помощью подтасованных сделок с недвижимостью. Мошенники нанимают бездомных или малоимущих лиц в качестве фиктивных заявителей на получение кредита в банках. В других случаях кредиты получают на основании поддельных паспортов. В рамках другого вида банковского мошенничества происходит захват счетов для проведения мошеннических сделок. Ипотечное мошенничество обычно связано с подделкой документов.

Число случаев ***мошенничества с субсидиями*** с годами неуклонно возрастает. В рамках мошенничества с субсидиями преступники подают фальшивые заявления на получение грантов ЕС или участие в тендерах. Как правило, такие заявления основываются на фальшивых декларациях, отчетах о ходе работ и счетах, которые используются для подтверждения государственных расходов или мошенническим образом полученных государственных тендеров и (или) субсидий. В интернет-объявлениях жертв приглашают открывать онлайн-торговые портфели, заманивая выгодой при открытии. Однако вскоре, изъяв средства, мошенники исчезают. Кроме того, в качестве инвестиционных возможностей рекламируют несуществующие виртуальные валюты.

Мошенничество с недоставкой — это вариант мошенничества с платежным поручением или авансовым платежом. Такие мошенники рекламируют или продают несуществующие товары, используя фиктивный интернет-магазин. В первые месяцы пандемии COVID-19 мошенники воспользовались высоким спросом на средства индивидуальной защиты и наборы для самостоятельного проведения тестов и недостаточным объемом их поставок. Число сайтов и аккаунтов социальных сетей, рекламирующих эти продукты в мошеннических целях, значительно выросло. Прибыли от подобных мошеннических схем были немалыми, среди пострадавших много коммерческих и бюджетных организаций, например больниц или клиник, размещавших заказы на поставку на сумму в несколько миллионов евро.

В рамках ***любовных афер*** мошенники связываются с потенциальными жертвами с целью воспользоваться финансами тех, кто действительно ищет любовь. Мошенники стараются постепенно втереться в доверие к жертве и вскоре начинают вытягивать личные

данные, например номера банковских счетов, банковских карт, или просить денег.

Мошенничество с фальшивым счетом, которое также называют ***мошенничеством с платежным поручением или мошенничеством со счетом-призраком***, — разновидность аферы с приобретением, в рамках которого на основе фальшивых счетов, выставленных потенциальным жертвам, мошенники требуют от них оплаты. Этот вид мошенничества основан на рекламных объявлениях на торговых интернет-сайтах.

Уклонение от уплаты пошлин на импорт товаров в ЕС отрицательно сказывается на финансовых интересах ЕС и негативно отражается на законопослушных компаниях, действующих на территории государств-членов. Из-за демпингового импорта создается недобросовестная конкуренция с законопослушными предприятиями, и главная составляющая в совершении мошенничества с НДС в каких бы то ни было целях — это технологии и цифровая инфраструктура. Криминальные структуры используют технологии для сокрытия своей преступной деятельности, например удаленные серверы и хранилища данных (в том числе облачные хранилища и серверы за пределами ЕС), платформы цифровых и альтернативных платежей, VPN-услуги, зашифрованные сообщения и разные приложения интернет-мессенджеров для смартфонов.

Криминальные структуры теперь могут создавать и управлять компаниями с помощью одного лишь устройства, находящегося в любой стране, вести торговлю и передавать документацию по интернету. Кроме того, сейчас есть бесплатное программное обеспечение для создания фальшивых счетов и банковских выписок. А из-за появления новых способов перевода денег, таких как альтернативные банковские платформы, а также сервисов электронных банковских платежей вычислить злоумышленников стало еще сложнее.

Преступники принимают меры, чтобы не дать себя обнаружить, например заменяют компании и их руководителей и используют новые технологии, чтобы оформлять компании и скрывать их владельцев. Примерами гибкости и приспособляемости криминальных структур, действующих в данной области преступной деятельности, являются ***использование альтернативных банковских платформ в карусельных мошеннических схемах и попытки внедрить гарантии исходных рынков***.

Жертвами организаторов договорных матчей все чаще становятся участники развивающегося ***рынка киберспорта***. Существуют показатели, которые свидетельствуют о манипуляциях

в киберспорте, среди них: необычный всплеск ставок и необычно крупные суммы ставок перед самым началом матчей.

Быстрое распространение сложных цифровых технологий и широкое использование социальных сетей и средств для обмена зашифрованными сообщениями открывает для организаторов ***незаконной перевозки мигрантов*** возможности передавать информацию о своих услугах, согласовывать действия между собой и искать жертв, избегая обнаружения правоохранительными органами. Структуры, занимающиеся незаконной перевозкой мигрантов, используют криптовалюты, и в ближайшем будущем объем их использования может увеличиться. Незаконные перевозчики часто пользуются цифровыми услугами и инструментами, например социальными сетями и мобильными приложениями, для вербовки, общения и совершения денежных переводов, встречи и передачи мигрантов, массовой мобилизации потоков мигрантов, обеспечения навигации на маршруте, обмена фото- и видеодокументов и билетов, а также отслеживания действий правоохранительных органов (по камерам видеонаблюдения и даже с дронов).

Продажа контрафактной продукции через интернет-сайты получила еще более широкое распространение и отражает возрастающую роль интернета как основной розничной площадки для легальной продукции и услуг. Благодаря интернет-торговле производители контрафакта получают прямой доступ к потребителям, сокращая таким образом число посредников и увеличивая охват. Большая часть розничной торговли контрафактной продукцией ведется в интернете, социальных сетях и на торговых площадках, а также на специализированных сайтах. Оценить спрос на контрафактную продукцию сложно, поскольку во множестве случаев потребители не знают, что приобретают контрафактный товар. Контрафактная продукция, как правило, производится за пределами ЕС и ввозится для распространения в магазинах, на рынках и в интернете. Контрафактные товары ввозятся готовыми к продаже и в виде заготовок. Объем импорта заготовок, этикетки и упаковка для которых ввозятся или изготавливаются отдельно, увеличился, поскольку сокращается риск обнаружения на границе. Большая часть торговли осуществляется в видимом секторе интернета. Однако некоторые фармацевтические продукты распространяются и через сайты даркнета.

Во время пандемии COVID-19 спрос на цифровой контент, как легальный, так и нелегальный, резко возрос. Ожидается, что ***распространение контента на физических носителях в ЕС полностью прекратится, поскольку его заменит более доступный***

цифровой контент. Для оплаты доступа к пиратскому контенту будут широко использоваться виртуальные валюты. Число легальных способов доступа к развлечениям в интернете увеличилось, и они стали дешевле для потребителей. Возможно, благодаря этому в будущем пиратский контент станет менее привлекательным.

Пиратское использование цифрового контента — это деятельность по нелегальному копированию и продаже цифрового контента, например музыки, книг, компьютерных программ и игр. Пиратство быстро эволюционирует одновременно с другими научно-техническими достижениями. ***Пиратство в настоящее время почти исключительно цифровое преступление***, поскольку деятельность по распространению физических копий аудиовизуального контента практически полностью исчезла.

Распространение поддельных денежных знаков также стало цифровым преступлением. В интернете рекламируют и продают банкноты разных валют и номиналов, материалы и оборудование для нелегального изготовления, пособия, обучающие, как изготавливать поддельные деньги, и информацию об элементах защиты.

Как противостоять кибермафии в России?

Главное направление — это разработка новых инструментов борьбы с киберпреступностью в рамках действующих национальных структур и подходов, при сохранении приоритета оперативно-розыскного воздействия.

В МВД России, например, разработана и активно применяется ***программа «Дистанционное мошенничество»***, с помощью которой выявляются серийные мошенничества, совершенные дистанционным способом. Благодаря эффективности использования подсистемы «Дистанционное мошенничество» выявлено более 324 тыс. признаков серийных преступлений. Эта программа дает возможность осуществлять сбор, систематизацию, обработку и анализ сведений, которые собираются в рамках расследования уголовных дел о преступлениях, совершенных дистанционным способом с использованием ИКТ. Программа позволяет фиксировать необходимые сведения с момента регистрации сообщения о таких преступлениях.

Е.Н. Яковец

О значении общих признаков «криминального» и «государственного» кибертерроризма для оперативно-розыскной, разведывательной и контрразведывательной деятельности

В современных условиях ускорения темпов научно-технического прогресса четко проявляются тенденции компьютеризации, создания разветвленных систем обработки данных, включающих в себя ЭВМ, информационные системы и компьютерные сети. Информатизация затрагивает практически все стороны государственной и общественной жизни, в связи с чем информационные ресурсы, системы обработки данных и информационно-телекоммуникационные сети становятся самым уязвимым звеном национальной инфраструктуры каждого государства.

Возможности современных информационных технологий активно пытаются использовать ОПГ, организованные преступные сообщества и преступники-одиночки, что приводит к появлению новых видов преступных деяний — киберпреступлений. Представители криминалитета осуществляют незаконное вмешательство в работу ЭВМ, систем и компьютерных сетей, осуществляют хищение, присвоение, вымогательство компьютерной информации, организуют удаленные атаки на информационные ресурсы, разрабатывают и закладывают компьютерные вирусы и т.д. По своему механизму, способам совершения и сокрытия эти виды преступлений имеют определенную специфику, характеризуются высоким уровнем латентности и низкой раскрываемостью.

Информационные технологии и компьютерные сети все активнее используются транснациональным террористическими и экстремистскими организациями с целью создания хаоса на мировой арене, что обусловило появление наиболее опасной разновидности компьютерной преступности — ***кибертерроризма***. Такие террористические организации, как «Аль-Каида», «Братья-мусульмане», «Имарат Кавказ», «Исламское государство»[1] и др., активно

[1] Организации, запрещенные в России.

используют возможности интернета. В виртуальном пространстве ими осуществляются информационные кибератаки, пропаганда экстремистских идей, расовой, религиозной и других форм нетерпимости, а также вовлечение в свои ряды новых членов, реализуются незаконные финансовые операции и т.д.

В современной юридической науке однозначного определения данного понятия не имеется. Обобщив точки зрения различных специалистов, можно сделать вывод, что *кибертерроризм* — это комплекс преднамеренных преступных деяний в киберпространстве, создающих угрозу безопасности личности, общества и государства, связанных с насилием или угрозой насилия, применяемыми негосударственными субъектами в отношении государств, международных организаций, хозяйствующих субъектов, объектов гражданской и военной инфраструктуры, политиков, других известных личностей, а также случайных лиц с целью оказания психологического воздействия на сознание людей в политических, социальных, религиозных или идеологических целях.

Переход некоторых хакерских преступных группировок на модель «криминал как услуга» укрепляет связи в цифровой среде террористов и обычных киберпреступников. Сегодня уже никого не удивишь тем, что представители террористических организаций в свободное от политической деятельности время осуществляют криминальные акции как в личных интересах, так и для обеспечения деятельности своих структур финансовыми ресурсами. В свою очередь, киберпреступники становятся все более «экономически завязанными» на террористические сети и, соответственно, оказываются уязвимы для шантажа и контроля[1]. Многие хакерские группы, такие как южно-славянская «Черная рука», пакистанская «G-Force» или палестинская «Unix Security Guard», не сделав ни единого выстрела, своими кибератаками нанесли серьезный ущерб институтам государственной власти ряда стран.

Потенциальная угроза кибератак со стороны международных террористов вырисовывается сегодня достаточно зримо. По данным экспертов, подобные нападения на государственные информационные системы, если они будут реализованы в широком аспекте на практике, могут иметь последствия, которые не менее опасны, чем традиционные террористические акты с использованием смертников, взрывчатки и т.п. Такие преступные деяния могут

[1] Оценка угроз организованной киберпрсетупности (IOCTA): доклад Европола от 28 сентября 2016 г. (цит. по: Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. М.: Норма, 2017. С. 287).

выводить из строя системы управления и функционирования АЭС и других важных объектов, нефте- и газопроводов, железных дорог, аэропортов, объектов водоснабжения и др. Например, в мае и июне 2002 г. действовавшие каждый индивидуально британский и австрийский хакеры взломали коды системы управления стратегическими ядерными силами и Центра космической разведки вооруженных сил США. Трудно представить последствия всех этих акций, если бы они были осуществлены в террористических целях.

Поэтому не случайно в качестве приоритетных направлений научно-технических разработок в области борьбы с террористической угрозой *Концепция противодействия терроризму в Российской Федерации*, утвержденная Президентом РФ 5 октября 2009 г.[1], называет создание и внедрение эффективных средств систем связи, отвечающих требованиям защищенности от компьютерных атак (пп. «в» п. 37).

С позиции уголовного законодательства кибертерроризм рассматривается мировым сообществом как особо тяжкое преступление против общественной безопасности и общественного порядка. В уголовно-правовой практике России деяния кибертеррористов в полной мере укладываются в рамки состава преступления, предусмотренного ст. 205 УК РФ («Террористический акт»). Следует кратко рассмотреть этот состав применительно к рассматриваемой специфике.

Объектом во всех преступлениях террористической направленности, в том числе совершаемых в киберпространстве, выступает общественная безопасность, базовые принципы и содержание деятельности по обеспечению которой устанавливает Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «*О безопасности*»[2]. К основным объектам безопасности в соответствии с положениями этого Закона относятся: личность — ее права и свободы; общество — его материальные и духовные ценности; государство — его конституционный строй, суверенитет и территориальная целостность (ст. 1).

Объективная сторона террористического акта, совершаемого кибертеррористами, заключается в альтернативных деяниях: 1) совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий; 2) угроза совершения указанных действий.

---

[1] Российская газета. 2009. 20 окт.

[2] Российская газета. 2010. 29 дек.

Взрыв, поджог и иные действия являются *способами* совершения преступления. Они могут быть инициированы различными факторами, в том числе путем кибернетической атаки на объекты критической информационной инфраструктуры (КИИ), «умные» города, «Интернет вещей» и др. Под *иными деяниями* понимаются общественно опасные действия, которые могут вызвать такие же последствия, как при взрыве или поджоге (например, провоцирование посредством применения интернет-технологий обвала горных пород, затопление объектов жизнеобеспечения путем разрушения ирригационных сооружений, плотин, шлюзов, отравление источников водоснабжения, запасов продовольствия, блокирование транспортных коммуникаций, средств связи, распространение радиоактивных, отравляющих веществ, эпидемий, эпизоотий и т.д.).

Значительный имущественный ущерб определяется с учетом стоимости и значимости уничтожаемого или повреждаемого имущества, других материальных ценностей. Однако определяющим при этом является то обстоятельство, насколько уничтожение и повреждение либо угроза этого были способны повлиять на устрашение населения, на решения органов власти или международных организаций изменить свою политику.

Субъективная сторона террористического акта в кибернетической сфере характеризуется умышленной виной в виде прямого умысла. Лицо осознает, что инициирует в помощью компьютерных технологий совершение взрыва, поджога или иных действий, устрашающих население и создающих опасность гибели человека, причинения значительного имущественного ущерба либо наступления иных тяжких последствий, либо создает угрозу совершения указанных действий, и желает наступления общественно опасных последствий. Обязательным признаком террористического акта в кибернетической сфере является *специальная цель* — воздействие на принятие решения органами государственной власти, местного самоуправления или международными организациями. Кибертеррористы могут требовать, например, выплаты значительных денежных сумм, передачи им партий оружия, прекращения проводимой государством контртеррористической операции на определенной территории, вывода с этой территории участвующих в такой операции войсковых формирований, освобождения задержанных в ходе операции соучастников террористов и т.д.

Субъектом преступления является вменяемое физическое лицо, достигшее возраста 14 лет.

К *квалифицирующим признакам* террористического акта, совершенного в кибернетической сфере (ч. 2 ст. 205 УК РФ), от-

носятся указанные выше деяния, которые: а) совершены группой лиц по предварительному сговору или организованной группой; б) повлекли по неосторожности смерть человека; в) повлекли причинение значительного имущественного ущерба либо наступление иных тяжких последствий.

Квалифицирующими признаками, фигурирующими в ч. 3 рассматриваемой статьи, являются деяния, предусмотренные ч. 1 и 2 рассматриваемой статьи, сопряженные: 1) с посягательством на объекты использования атомной энергии либо на совершение деяний, сопряженных с использованием ядерных материалов, радиоактивных веществ или источников радиоактивного излучения либо ядовитых, отравляющих, токсичных, опасных химических или биологических веществ; 2) с умышленным причинением смерти человеку.

Кибертерроризм с момента своего зарождения стал стремительно обретать характер транснациональной, глобальной опасности. Генеральная Ассамблея ООН еще в резолюциях более чем 20-летней давности, посвященных данной проблеме, — 53/70 от 4 декабря 1998 г. и 54/49 от 1 декабря 1999 г. — поставила вопрос о целесообразности разработки международных принципов, направленных на усиление безопасности глобальных информационных и телекоммуникационных систем, борьбы с информационным терроризмом и преступностью.

23 ноября 2001 г. представители стран — членов Совета Европы, США, Канады, Японии и ЮАР подписали *Конвенцию о преступности в сфере компьютерной информации*[1]. В Совете ЕС было создано специальное «Агентство информационной безопасности», контролирующее реализацию его положений.

Противостоять деяниям злоумышленников, как известно, можно с использованием законодательных, организационных и технических мер. Именно на последние сделали ставку крупнейшие мировые провайдеры интернет-услуг. В частности, 28 марта 2005 г. они объявили о заключении глобального антихакерского альянса. В его рамках компании создали систему раннего оповещения о хакерских атаках в интернете[2].

5 июля 2011 г. в Лондоне был создан *Международный альянс обеспечения кибербезопасности* (*The International Cyber Security*

---

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // ИПП «Гарант». URL: https://base.garant.ru/4089723/ (дата обращения: 22.03.2021).

[2] *Акопов Г.Л.* Правовая информатика: современность и перспективы: учеб. пособие. Ростов н/Д, 2005. С. 218.

Protection Alliance — ICSPA). По данным телекомпании Би-би-си, новая структура, «объединившая правительства, международный бизнес и правоохранительные органы, включая Европол», предназначена для борьбы с киберпреступностью в глобальных масштабах. Данная организация является некоммерческой. Ее финансирование осуществляется ЕС и рядом правительств других стран (в их числе — Австралия, Великобритания, Канада, Новая Зеландия, США), а также компаниями частного сектора[1].

Международные нормативные правовые акты в сфере противодействия киберпреступности и кибертерроризму достаточно хорошо известны и надлежащим образом систематизированы[2]. Ограничимся лишь некоторыми из них, например Резолюцией Генассамблеи ООН, принятой в 2019 г. по инициативе России. Этот документ призывает соблюдать принципы суверенного равенства и невмешательства во внутренние дела государств. Россия полагает, что Конвенция о преступности в сфере компьютерной информации, разработанная в конце 1990-х гг., не в состоянии регулировать многие современные отношения в данной сфере, а также противостоять кибертерроризму. Она допускает возможность нарушения принципов государственного суверенитета и невмешательства во внутренние дела других государств и по-прежнему создает угрозу легитимизации доступа специальных служб ограниченной группы стран к бесконтрольному сбору персональных данных пользователей со всего мира, а также способствует сохранению установленной рядом государств тенденции консолидации их технических достижений в информационном пространстве и сохранения цифрового разрыва между развитыми и развивающимися странами[3].

Обеспокоенность руководства России на этот счет вполне понятна, поскольку хакерские методы могут с успехом использоваться не только террористическими организациями и злоумышленниками-одиночками, но и представителями силовых структур

---

1 См.: В Лондоне создан Международный альянс обеспечения кибербезопасности // Вести.ру. URL: http://www.vesti.ru/doc.html?id=499251 (дата обращения: 14.07.2011).

2 См., например: Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. М.: Норма, 2017.

3 См.: Доклад Генерального секретаря ООН по Резолюции Генеральной Ассамблеи ООН от 30 июля 2019 г. № 73/187 «Противодействие использованию информационно-коммуникационных технологий в преступных целях». С. 74 // Организация Объединенных Наций. URL: https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf (дата обращения: 11.03.2021).

развитых в кибернетическом отношении стран в ходе так называемых «гибридных войн»[1].

За последние несколько лет было высказано немало опасений по поводу того, что террористы могут начать эффективные кибератаки против КИИ различных государств. Однако, несмотря на то что онлайн-пропаганда террористов выглядит весьма активной и они неплохо используют возможности шифрованных мессенджеров для коммуникаций, их хакеры пока еще недостаточно сильны в том, что касается использования продвинутого софта для осуществления разрушительных кибератак. Они не только не используют многофункциональные шпионские и боевые программы, но и продолжают закупать услуги хостинга, арендуют ботнеты для DDoS-атак и используют другой устаревший софт, характерный для подростков и одиночных преступников[2].

На этом фоне большинство развитых стран Запада формируют кибервойска и ведут работу по использованию виртуального пространства для достижения собственных геополитических целей, мотивируя это обеспечением кибербезопасности[3].

Еще в 2011 г. Президент США определил 10 экстренных мер, необходимых для реализации стратегии кибербезопасности, в частности:

1) учредить подразделения киберполиции, которые отвечали бы за обеспечение кибербезопасности;

2) подготовить обновленную национальную стратегию по обеспечению информационной и коммуникационной инфраструктуры;

3) передать контроль за кибербезопасностью под прямое управление Президента США и установить показатели, определяющие ее эффективность;

4) обеспечить конфиденциальность и гражданские свободы в рамках деятельности национальной секретной службы кибербезопасности;

---

[1] См.: Третья мировая на пороге. Какая она?: интервью генерал-полковника, специалиста в области геополитики, конфликтологии, международных отношений и военной истории, президента Академии геополитических проблем Л.Г. Ивашова главному редактору газеты «Аргументов недели» А. Угланову // Аргументы недели. 2021. 10–16 февр. № 5 (749). С. 6.

[2] *Жданов Ю.Н.*, *Овчинский В.С.* Киберполиция XXI века. Мировой опыт. М.: Международные отношения, 2020. С. 99.

[3] *Акопов Г.Л.* Хактивизм как неотъемлемый элемент современных информационных войн // Национальная безопасность. 2014. № 3 (32). С. 438–444.

5) провести межведомственный нормативно-правовой анализ в целях определения приоритетных вопросов в области кибербезопасности;

6) инициировать национальную информационно-просветительскую кампанию содействия кибербезопасности;

7) разработать единый международный план действий по обеспечению кибербезопасности и укрепления международных партнеров США;

8) подготовить ответ кибератакам: инициировать план действий и начать диалог для укрепления государственно-частного партнерства;

9) разработать основу для исследований применения новейших технологий, которые могли бы обеспечить повышение безопасности, надежности и устойчивости работы цифровой инфраструктуры;

10) принять протокол кибербезопасности, основанный на стратегии управления и обеспечения конфиденциальности технологий повышения национальной безопасности[1].

Таким образом, методы ведения кибернетической войны, сходные до степени смешения с методами, практикуемыми хакерами, начали в тот период активно заимствоваться и использоваться силовыми ведомствами отдельных государств. Причем, что характерно, подобные действия рассматриваются последними как оборонительные и их реализация предусматривается военными доктринами этих государств. Взять, к примеру, деятельность в этом направлении англоязычных стран.

Центр передового опыта совместной киберзащиты НАТО (*NATO Cooperative cyber defense centre of excellence, NATO CCDCOE*) опубликовал 30 октября 2020 г. отчет «Альянс “Пять глаз” и наступательные возможности в киберпространстве: реализация Инициативы киберсдерживания». Этот документ содержит анализ положений ряда рассекреченных нормативных правовых актов. В нем отмечается, что более 30 государств мира развивают наступательные возможности в киберпространстве и делают это по-разному, что приводит к разногласиям на межгосударственном уровне. Взгляды государств — членов ООН на концепцию «милитаризации» киберпространства расходятся. Некоторые из них, такие как Россия, Китай и Иран, *призывают к запрету наступательных операций*

[1] Cybersecurity // Официальный сайт Президента США. URL: http://www.whitehouse.gov/administration/eop/nsc/cybersecurity (дата обращения: 15.03.2021).

в киберпространстве и отказываются признавать тот факт, что они сами осуществляют такую политику, считают авторы отчета.

Западные страны, в отличие от «коварной», по их мнению, России выступают за признание и открытое обсуждение развития наступательных возможностей в киберпространстве с соблюдением принципа «прозрачности», который гарантирует предсказуемость и стабильность в этой области. Развитие наступательных возможностей в этой сфере, если они согласуются с действующими нормами международного права, для западных государств является само собой разумеющимся. Причем США и весь «коллективный Запад» полагают, что действующих норм международного права для обоснования боевых действий в киберпространстве вполне достаточно.

В указанном отчете говорится также о том, каким образом каждое из государств — членов разведывательного альянса англоязычных государств «Пять глаз» (Five Eyes) реализует политику наступательных возможностей в киберпространстве. Кратко рассмотрим их намерения в данном аспекте.

Действия *США* в этом плане основываются на реализации Инициативы киберсдерживания (*Cyber-Deterrence Initiative, CDI*), которая впервые была представлена в 2019 г. в Национальной киберстратегии США, предполагающей их взаимодействие со странами-союзниками для отражения кибернападения. В различных американских нормативных правовых актах, касающихся данной проблематики, используются термины, регламентирующие политику наступательных возможностей в киберпространстве, описывается порядок принятия решений, определяются организационная структура уполномоченных органов власти и правила их взаимодействия.

Пентагон классифицирует кибератаки со стороны иностранных государств как акты агрессии и предусматривает возможность применения в ответ военной силы. США считают себя вправе отвечать реальными военными ударами на возможные атаки в киберпространстве. Об этом говорится в докладе «Иностранные шпионы, крадущие экономические секреты США в киберпространстве», который Пентагон подготовил для американского Конгресса[1].

Согласно ст. 1642 Закона об обеспечении национальной безопасности на 2019-й финансовый год, министерство обороны США

[1] *Кондрашов А.* США в ответ на кибератаки других стран могут нанести реальный военный удар // Аргументы недели. 2021. 16 марта. URL: https://argumenti-ru.turbopages.org/argumenti.ru/s/espionage/2021/03/713905 (дата обращения: 20.03.2021).

наделено полномочиями по проведению наступательных операций в киберпространстве против четырех государств — России, Китая, Северной Кореи и Ирана. Причем американцы намерены использовать кибератаки как законное средство реагирования на нарушения действующих норм международного права. США провозглашают право действовать в этом ключе без согласования с другими государствами.

Великобритания. В положениях Национальной стратегии с сфере кибербезопасности на 2016–2021 гг. говорится, что эта страна намерена активно противостоять злоумышленникам в киберпространстве, бороться с их инфраструктурой, делать все возможное для наказания преступников в соответствии с международным правом.

Центр правительственной связи Великобритании (*Government Communications Headquarter, GCHQ*) отмечает, что существующая практика применения международного права в киберпространстве недостаточна, в связи с чем толкование норм международного права в этой сфере в разных странах может значительно различаться. Как и США, Великобритания полагает возможным проводить операции в киберпространстве без согласования с другими государствами.

Австралия. В этой стране с 2016 г. действует Военная доктрина ведения операций в киберпространстве, устанавливающая понятия «наступательные возможности в киберпространстве», «пассивная» и «активная» киберзащита, а также «разрешающая операции государства в киберпространстве в ответ на действия злоумышленников». Под наступательными возможностями понимаются полномочия вооруженных сил Австралии атаковать инфраструктуру враждебной стороны с целью достижения целей, поставленных перед вооруженными силами для обеспечения безопасности государства.

Наступательные возможности в киберпространстве австралийцы планируют использовать как альтернативный способ реагирования на киберугрозы злоумышленников наряду с дипломатическими и экономическими мерами.

Канада. Впервые Канада официально заявила о готовности к применению наступательных возможностей в киберпространстве в 2017 г. в рамках Доктрины оборонной политики страны. В ней говорится, что действия Канады в киберпространстве будут становиться активнее. Против злоумышленников будут проводиться кибероперации. Вооруженные силы Канады должны обеспечивать наступательные возможности в киберпространстве.

Закон об обеспечении безопасности связи 2019 г. наделил Управление по обеспечению безопасности связи полномочиями для

проведения наступательных операций в киберпространстве за пределами Канады. Авторы отчета констатируют, что правительство Канады пока не конкретизировало положения данного закона.

Новая Зеландия. Меморандум о стратегии оборонительной политики 2018 г. признает необходимость расширения возможностей вооруженных сил Новой Зеландии в киберпространстве. Согласно Стратегии кибербезопасности Новой Зеландии, принятой в 2019 г., эта страна намерена всеми силами способствовать предотвращению вредоносной киберактивности, в том числе задействуя специальную группу реагирования на киберугрозы. В документе перечислены исключительно защитные механизмы, а не военные наступательные возможности в киберпространстве, и это выделяет Новую Зеландию среди государств — членов альянса «Пять глаз». Тем не менее авторы отчета полагают, что законодательство Новой Зеландии в рассматриваемом аспекте соответствует политике альянса.

Таким образом, позиция государств — членов альянса «Пять глаз» заключается в необходимости оперативного реагирования на нарушения их кибербезопасности, в том числе с помощью ответных кибератак и иных боевых действий. Наряду с этим отмечается, что основными задачами стран альянса на сегодняшний день являются подписание межгосударственного соглашения об общих принципах и правилах реализации политики наступательных возможностей в киберпространстве, повышение уровня прозрачности такой политики и обеспечение ее соответствия действующим нормам международного права[1], хотя от такого диалога со своими политическими оппонентами эти страны упорно отказываются.

Из приведенных материалов видно, что именно англосаксы совместно с другими странами НАТО, примерив на себя «тогу миротворцев», активно продвигают возможность использования киберпространства для ведения агрессивных войн с использованием сил, средств и методов, заимствованных у кибертеррористов. Причем врагом номер один для них в этом плане является Россия, представляющая наибольшую угрозу национальной безопасности Америки и опережающая по степени опасности КНДР с его ядерным ору-

[1] *Федотов А.* Альянс «Пять глаз» и наступательные возможности в киберпространстве — отчет НАТО // D-russia. ru. 2020. 11 нояб. URL: https://d-russia.ru/aljans-pjat-glaz-i-nastupatelnye-vozmozhnosti-v-kiberprostranstve-otchjot-nato.html (дата обращения: 09.03.2021).

жием и Исламское государство[1] с его джихадистами[2]. Основания и поводы для «наказания» нашей страны коллективным Западом изыскиваются уже давно, и проба сил в этом направлении имела место не вчера.

Предпосылкой для успешной реализации агрессивных замыслов противников России является ее вре́менная технологическая зависимость от зарубежных разработчиков компьютерной техники и программного обеспечения, которая приводит к появлению в нашей информационной инфраструктуре множества уязвимых мест, обусловливающих возможность вторжения в нее вероятного противника. Подобные уязвимости могут использоваться для реализации массированных групповых и одиночных программных ударов, специальных операций и систематических действий по выявлению наиболее важных объектов КИИ нашей страны с целью заблаговременного установления над ними скрытого контроля и последующего выведения их из строя. Не исключаются и более пагубные сценарии, например ядерный взрыв на АЭС или создание транспортного коллапса на железнодорожных магистралях и в аэропортах; полный паралич банковской системы или химическое заражение окружающей среды и т.п. На языке военных средства информационного воздействия, используемые против России потенциальным противником, имеют вполне конкретное название — «программно-компьютерная атака» или «оружие направленной энергии», которые в более широком контексте именуются «некинетическое оружие» или «кибероружие».

Хорошо известно, что разведслужбы США используют современные компьютерные технологии для тотальной слежки за всем миром, нередко оказывая при этом соответствующие услуги американским корпорациям в борьбе с конкурентами. Причем имеются примеры и обратного характера, подчас стирающие грани между политическим, военным, экономическим шпионажем и своего рода «неототалитаризмом». К примеру, французские спецслужбы еще 20 лет назад опубликовали доклад, в котором утверждалось, что компьютерный гигант «Майкрософт» сотрудничает со спецслужбами США. Создаваемые этой компанией программы позволяют следить за действиями пользователей с помощью специальных «закладок», которые при необходимости могут не только «прочитать»

---

[1] Организация, запрещенная в России.

[2] Кто главный враг Запада: Россия или терроризм? // ОБЗОР.PRESS. Переводы иностранной прессы. 2016. 23 марта. URL: https://obzor.press/press/18386-kto-glavnyij-vrag-zapada-rossiya-ili-terrorizm (дата обращения: 17.03.2021).

нужную информацию, но и вывести из строя те или иные аппаратно-программные средства[1]. К слову сказать, программы «Майкрософт» до сих пор установлены у подавляющего большинства компьютерных пользователей.

Разоблачения международной некоммерческой организация «WikiLeaks» и Э. Сноудена свидетельствуют о том, что разведывательные органы США и их союзников ведут наблюдение за миллиардами людей по всему миру, в том числе с помощью различных электронных устройств, используемых в бытовых целях. Телевизоры, смартфоны и даже антивирусный софт — все это уязвимо для взлома ЦРУ и АНБ. Данные возможности включают записи звуков, изображений и приватных текстовых сообщений пользователей, даже если они прибегают в ходе общения к шифрующим приложениям. Все эти меры направлены на тотальный сбор информации, в том числе и с целью нанесения с помощью кибероружия последующих ударов в виртуальном пространстве, представляющих собой по сути хакерские атаки на стратегические объекты вероятного противника. Вполне очевидно, что подобные деяния, совершаемые представителями спецслужб западных государств, выходят за рамки обычной общеуголовной практики и обретают черты *государственного кибертерроризма*.

Таким образом, как справедливо отмечал профессор О.В. Дамаскин, «кое-где информационный терроризм стал элементом государственной политики. В некоторых странах активно ведутся работы над компьютерными программами, являющимися информационным оружием. Причем объектами для такого оружия все чаще становятся отдельные личности, социальные группы, принимающие решения, а не только массы и государственные структуры, как это было не так давно. Иными словами, избирательность этого оружия растет, именно люди, в первую очередь высокопоставленные, являются теперь главной целью в информационных войнах, и их принуждают к выбору необходимых противнику решений. Информационное воздействие на государство, общество, отдельно взятого человека в конечном счете оказывается более эффективным и экономичным, чем политическое, экономическое и даже силовое, военное»[2].

В рамках тектонических сдвигов, происходящих на международной арене, страны Запада постоянно обвиняют в хакерских

[1] См.: *Бовт Г.* Большой Брат по имени Эшелон // Известия. 2000. 24 февр.

[2] *Дамаскин О.В.* Россия в современном мире: проблемы национальной безопасности: монография. М.: Флинта; Наука, 2007. С. 267.

атаках на их информационные ресурсы Россию. Консультанты Белого дома даже включили нашу страну в список «государств-хакеров». Можно назвать следующие наиболее громкие киберпреступления, в совершении которых за последние годы обвиняли российских хакеров:

- 2007 г. — атака на правительственные сайты Эстонии;
- 2008 г. — атака на официальный сайт президента Грузии;
- 2009 г. — отключение от интернета Киргизии;
- 2014 г. — атака на государственные сайты Украины; вмешательство в выборы президента этой страны;
- 2015 — взлом электронной почты депутатов Бундестага в ФРГ; отключение энергосетей на Украине;
- 2016 г. — взлом серверов Национального комитета Демократической партии США; взлом почты Хиллари Клинтон; вмешательство в выборы президента США; вмешательство в референдум о выходе Великобритании из ЕС; похищение внутренних документов Всемирного антидопингового агентства[1];
- 2017 г. — попытка сорвать выборы во Франции; использование вируса NotPetya в серии атак с причинением ущерба США в размере свыше 1 млрд долл., а в целом по всему миру — на сумму около 10 млрд долл.;
- 2018 г. — атаки с использованием целевого фишинга в отношении Организации по запрещению химического оружия и Лаборатории оборонной науки и технологий Великобритании; использование вредоносной программы Olympic Destroyer, предназначенной для отключения интернет-соединений во время церемонии открытия зимних Олимпийских игр в 2018 г. (г. Пхёнчхан, Южная Корея)[2];
- 2020 г. — атаки на организации, участвовавшие в разработке вакцины от COVID-19 в Великобритании, США и Канаде[3]; вмешательство в президентские выборы в США; взлом информаци-

---

1 Большая игра. Выпуск от 11 марта 2021 г. // Первый канал. URL: https://www.1tv.ru/shows/big-game/vypuski/bolshaya-igra-vypusk-ot-11-03-2021 (дата обращения: 12.03.2021).

2 *Саенко Л.* Русских хакеров обвинили по полной программе. Власти США насчитали ущерб от их действий на $10 млрд // Коммерсантъ. 2020. 19 окт. URL: https://www.kommersant.ru/doc/4539225 (дата обращения: 14.03.2021).

3 *Вахрушева Я.* Российских хакеров снова обвинили в атаках — на этот раз на вакцину от COVID-19 // 5 канал. 2020. 16 июля. URL: https://www.5-tv.ru/news/304167/rossijskih-hakerov-snova-obvinili-vatakah-naetot-raz-navakcinu-otcovid19/ (дата обращения: 14.03.2021).

онных систем Министерства финансов США и Национального управления по телекоммуникациям и информации с целью похищения данных[1]; и др.

В последних случаях Вашингтон возлагает ответственность за кибератаки на хакерскую группировку «Cozy Bear», работающую якобы на российскую Службу внешней разведки. Позже выяснилось, что для взлома федеральных сетей хакеры использовали уязвимость в программном обеспечении компании «SolarWinds», являющейся подрядчиком «Microsoft». Президент «Microsoft» Брэд Смит на слушаниях в сенате США в феврале 2021 г. заявил, что у компании есть «солидные» доказательства причастности Москвы к взлому американских сетей.

Представители руководства нашей страны опровергают причастность России к произошедшему и заявляют, что не поддерживают киберпреступность.

Эту позицию твердо отстаивал президент В.В. Путин на саммите с президентом США Джо Байденом 16 июня 2021 г. в Женеве, где вопросам кибербезопасности уделялось первостепенное внимание.

Российская сторона всегда обращает внимание американцев на перевернутое представление об угрозах кибертерроризма. Подобные угрозы возникают гораздо чаще не от России, а от самих Соединенных Штатов. Так, в начале марта 2021 г. газета «The New York Times» со ссылкой на информированные источники объявила, что власти США в ближайшие три недели предпримут несколько кибератак против России в ответ на крупномасштабный взлом американских правительственных сетей, обнаруженный в конце 2020 г.[2] Данное сообщение представляет особый интерес с точки зрения формулирования сущности и содержания *государственного кибертерроризма*. Попробуем определить это понятие, но не с помощью дефиниции, а путем перечисления его основных признаков.

Итак, хакерские атаки, как пишет газета, *будут скрытными и незаметными для остального мира*, *но «очевидными для российской разведки*, *вооруженных сил и Президента Владимира Путина»*. Это означает следующее: в данном конкретном случае кибератаки носят

---

[1] *Назарова А.* «Российских хакеров» бездоказательно обвинили во взломе системы минфина США // Взгляд. Деловая газета. 2020. 14 дек. URL: https://vz-ru.turbopages.org/vz.ru/s/news/2020/12/14/1075576.html (дата обращения: 14.03.2021).

[2] *Котляр М.* NYT сообщила о готовящейся в США серии кибератак на Россию // РБК. 2021. 8 марта. URL: https://www.rbc.ru/politics/08/03/2021/6045814a9a7947d87795a619 (дата обращения: 09.03.2021).

демонстративный характер, поскольку они анонсированы через СМИ, однако подобные действия могут осуществляться и без предварительного предупреждения, т.е. тайно.

Инициаторы их проведения рассчитывают оказать *политическое давление* на определенных лиц из числа руководства нашей страны. К таковым относятся руководители СВР и Минобороны России, а также лично Президент РФ В.В. Путин. В своем скандальном интервью от 17 марта 2021 г. телеканалу «ABC News» президент США Джо Байден продублировал эти угрозы, пообещав, что «Владимир Путин "заплатит" за вмешательство в американские президентские выборы», и допустив откровенно оскорбительные выпады в отношении нашего Президента, "хозяин" Белого дома, однако, не пояснил, в чем именно будет заключаться обещанная им "расплата"»[1].

Кибератаки, планируемые в отношении России, по словам газеты «The New York Times», *будут проводиться в сочетании с дополнительными экономическими санкциями*. Одних лишь экономических мер Западу явно не хватает, поэтому, чтобы более основательно наказать нашу страну, он предпринимает дополнительные шаги, в том числе реализуемые через киберпространство.

Причем все это агрессивное поведение имеет место *на фоне концентрации натовских войск* вдоль западных российских границ, нагнетания напряженности в Донбассе, притязаний на северные акватории России в тающих льдах Арктики, наращивания противостояния в космосе и др. То есть возможные кибердудары сочетаются не только с экономическими, но и с *военными мерами давления* на нашу страну, а также с активной *антироссийской пропагандой*.

Таковы основные признаки государственного кибертерроризма, угрозу воздействия которого испытывает на себе Россия.

Администрация Байдена *одержима идеями насаждения во всем мире американского образа жизни* с его однополыми браками, гипертрофированной толерантностью по отношению к различным «меньшинствам», весьма специфическими духовными ценностями и предпочтениями, движением «Black Lives Matter» и культивированием доллара. Как известно, для того чтобы в их собственной стране не было инфляции, власти США постоянно расширяли и расширяют зону хождения своей валюты, подсаживая на «долларовую иглу» весь остальной мир. Направляя инфляционные деньги в другие страны, они таким образом осуществляют экспорт своей

[1] *Наумов А.* «Он заплатит». Джо Байден ответил утвердительно на вопрос, считает ли он Владимира Путина убийцей // Коммерсант. 2021. 17 марта. URL: https://www.kommersant.ru/doc/4731349?u tm_source=yxnews&utm_medium=desktop (дата обращения: 17.03.2021).

собственной инфляции за счет дополнительной эмиссии местных валют[1]. Американские представления о демократии эти люди *собираются нести всему остальному миру, насильно насаждая в нем свои порядки и свои экономические интересы, в том числе и с помощью кибероружия.*

Не следует полагать, что американцы в киберпространстве являются исключительно потерпевшей стороной. Они постоянно увеличивают число кибератак на КИИ России с территорий Северной Америки и Европы, включая недружественные России страны ближнего зарубежья. Только в отношении объектов военной инфраструктуры нашей страны таких акций за последнее время было проведено тысячи, и их количество год от года растет. В 2019 г. зафиксировано около 20 тыс., в 2020 г. — около 30 тыс., за 3 месяца 2021 г. — свыше 10 тыс. Соответственно возрастает и интенсивность проведения этих акций: в 2019 г. — 1600, в 2020 г. — 2500, в 2021 г. — около 3000 кибервторжений в месяц[2].

Таким образом, за последнее время наблюдается переход конкуренции в киберпространстве (как, впрочем, и в реальном мире) на качественно новый уровень: теперь это *противоборство, предполагающее нанесение противнику ощутимого ущерба.* Безусловно, данное обстоятельство повлечет за собой существенное повышение уровня международной конфронтации, которое приведет к стиранию грани между войной и миром. В подобной ситуации можно и не заметить, как «холодная» война перерастет в «горячую». Тем более что в киберсфере на сегодняшний день не имеется никаких регуляторных договоренностей между странами, а в Военной доктрине РФ, как и у ее оппонентов, содержатся положения, гарантирующие нанесение ответных ударов по агрессорам[3].

Как известно, каждое государство вправе осуществлять разведывательную и контрразведывательную деятельность, и ничего необычного в этом нет. Подобные действия могут носить нелегальный характер либо осуществляться под прикрытием определенных официальных структур. Представители противоборствующих разведывательных служб с целью сбора информации проникают на чужую

---

1 Бесценный доллар: фильм Ильи Колосова // YouTube. URL: http://yandex.ru/video/search?text=бесценный%20доллар%20смотреть%20онлайн&where=all&filmId=JaxZIOeas3M (дата обращения: 23.03.2021).

2 Большая игра. Выпуск от 11 марта 2021 г. // Первый канал. URL: https://www.1tv.ru/shows/big-game/vypuski/bolshaya-igra-vypusk-ot-11-03-2021 (дата обращения: 12.03.2021).

3 См.: пп. «у» п. 21 Военной доктрины Российской Федерации, утв. Президентом РФ 25 декабря 2014 г. № Пр-2976 (Российская газета. 2014. 30 дек.).

территорию и в то же время защищают свои собственные информационные ресурсы от аналогичных действий противника. Так было, есть и будет. Это аксиома разведывательной и контрразведывательной деятельности. Помимо агентурной разведки в эпоху развития научных достижений широко практикуется и разведка техническая (ТР), которая классифицируется по видам, решаемым задачам и используемым в качестве источников информации физическим полям исследуемых объектов.

По *видам* ТР подразделяется на космическую, воздушную, морскую и наземную, т.е. по месту размещения аппаратуры. По *решаемым задачам* различают стратегическую, оперативную и тактическую ТР. Основу классификации ТР по *информационным физическим полям* составляют физические принципы, используемые при разработке разведывательной спецтехники. В соответствии с этим подходом ТР подразделяется на оптическую (ОР), оптико-электронную (ОЭР), радиоэлектронную (РЭР), гидроакустическую (ГАР), акустическую (АР), химическую (ХР), радиационную (РДР), сейсмическую (СР), магнитометрическую (ММР) и *компьютерную разведку* (КР).

В XXI в. такие разведсведения с успехом получают специалисты-«технари», к числу которых относятся и киберразведчики, «выуживающие» тайны из компьютеров потенциального противника. Для этого пересекать чужие границы им не требуется. Соответственно, все те действия в киберпространстве, как реальные, так и мнимые, в которых огульно обвиняют Россию, целиком укладываются в концепцию современной *киберразведывательной деятельности*.

Вполне закономерно, что заимствование определенных данных в ходе осуществления киберразведки может быть сопряжено с нанесением вероятному противнику некоторого материального ущерба, поскольку любая информация обладает соответствующей ценностью или потребительской стоимостью, и в отдельных случаях ее можно рассматривать как *товар*[1]. Цена информации, как и любого товара, складывается из ее себестоимости и прибавочной стоимости (прибыли). Однако нанесение в мирное время в ответ на хищение информации кибердударов по своим оппонентам, предполагающих причинение крупного материального ущерба, воз-

[1] Подробнее см.: *Яковец Е.Н.* Основы правовой защиты информации и интеллектуальной собственности: учеб. пособие. 2-е изд., доп. и перераб. М.: Юрлитинформ, 2013. С. 10–20.

можную гибель людей и дестабилизацию жизни населения целых стран, — это уже фактически ***начало открытой кибервойны***.

Ситуация в этой сфере осложняется еще и тем, что достоверно установить субъектов разведывательной деятельности в киберпространстве чрезвычайно сложно, если вообще возможно, а вся политика «коллективного Запада» в отношении России традиционно строится на принципе, который можно выразить англоязычным словосочетанием «highly likely» («с высокой степенью вероятности» или просто «весьма вероятно»). Другими словами, речь идет о событиях, в которых нет стопроцентной уверенности.

Вполне возможно, что, например, вторжение в американское киберпространство могли осуществить какие-то другие хакеры, например последователи Дж. Ассанжа в отместку за нечеловеческое обращение с ним западного правосудия. «WikiLeaks», как известно, это не только Ассанж. Говорят, у главного инсайдера мира более четырех детей. Но на самом деле их сотни, а может и тысячи. Это все те, кто работает на «WikiLeaks», «Anonymous» и другие хакерские организации, взламывающие сети не ради наживы, а ради правды.

В качестве примера можно привести кибератаку, предпринятую на серверы Пентагона, НАСА и нескольких университетов США в конце 1990-х гг., получившую название «Лабиринт лунного света». Некоторые специалисты полагают, что инициатором ее проведения явился Китай. В середине нулевых годов ударам хакеров подверглись НАСА и три американские фирмы, имеющие отношение к оборонной промышленности. Эта операция под названием «Титановый дождь» также, по мнению американцев, была организована Китаем. Однако официально причастность этой страны к данным акциям так и не была подтверждена[1].

Кстати, практически одновременно с анонсированным кибернаступлением на Россию в Америке вновь проявился «китайский след». Агентство «Bloomberg», опять же «highly likely», сообщило, что мартовский взлом почтовых серверов «Microsoft», который затронул около 60 тыс. организаций по всему миру и превратился в глобальный кризис кибербезопасности, осуществлен китайскими хакерами. Американцы отмечают, что эта акция, как и атака на системы компании «SolarWinds», в совершении которой обвиняют россиян, несет в себе те же вызовы, хотя мишени и методы существенно различаются.

---

[1] См.: *Писаренко Д.* Кибервойны. Одной клавишей компьютера можно уничтожить страну // Аргументы и факты. 2011. № 36. С. 40.

По их словам, как и россияне, китайские хакеры начали свою кампанию против «Microsoft» с компьютерных серверов — облачных сервисов, которые они арендовали под чужими именами в США. Обе страны знают, что американский закон запрещает разведывательным агентствам следить за системами, находящимися в Соединенных Штатах, и хакеры воспользовались этой лазейкой. «Китайские хакеры, очевидно, потратили некоторое время, чтобы изучить правовую подоплеку, и выяснили, что, если они будут действовать изнутри США, лучшие федеральные охотники за угрозами окажутся вне игры», — заявил Том Бёрт (Tom Burt), возглавивший расследование хакерской атаки в компании «Microsoft».

Именно поэтому в случае с атакой на системы «SolarWinds» и атакой китайских хакеров американские разведывательные агентства, очевидно, упускали из виду свидетельства того, что происходило, пока их не заметила частная компания, которая и подняла тревогу.

Без сомнения, американские чиновники задумались над тем, стоит ли им принимать ответные меры против Китая. Ведь США могут оказаться в таком положении, когда им придется вступить в потенциально опасный конфликт с двумя своими крупнейшими противниками, обладающими ядерным оружием. К тому же Китай является важнейшим торговым партнером западных стран, и лишаться китайского рынка американцы не торопятся. За последние годы китайцы значительно преуспели в развитии IT-технологий и в ближайшее время намерены полностью избавиться от иностранной зависимости в данной области. Отряды китайских хакеров представляют собой единую стратегическую силу, аналогичную Киберкомандованию США. Самые важные хакерские операции проводятся Министерством государственной безопасности — ведущим разведывательным агентством Китая, на которое работает обширная сеть «подрядчиков». Помимо этого Пекин начал накапливать так называемые эксплойты нулевого дня — уязвимости, о которых создателям программного обеспечения пока ничего не известно и для которых пока нет «заплаток»[1]. Так что обострять конфронтацию с Китаем в киберпространстве американцы явно не желают, переключая весь свой негативный запал на Россию.

Как уже подчеркивалось выше, опасность данной ситуации усугубляется тем, что в военных доктринах и России, и США,

[1] *Сангер Д., Барнс Дж., Перлрот Н.* The New York Times (США): готовясь выступить с ответными мерами против России, США столкнулись с очередной хакерской атакой китайцев // Иносми. ру. URL: https://inosmi.ru/politic/20210308/249284861.html (дата обращения: 12.03.2021).

и Китая, а также других стран мира, которые имеют современные вооруженные силы, угрозы безопасности, исходящие от кибернетического и обычного оружия, не разграничиваются. У большинства из них на этот случай предусмотрена возможность военного ответного удара на кибератаку, в том числе с использованием ядерного оружия, если таковым они располагают. Поэтому в условиях жесткой конфронтации между отдельными государствами и при весьма ограниченном уровне диалога между их руководителями очень сложно будет разобраться, идет ли речь о начале реальных боевых действий или только об их имитации.

В рассматриваемом контексте следует обозначить ряд важнейших проблем в данной области, связанных с обеспечением безопасности отечественной виртуальной среды.

Практически все важнейшие хозяйствующие субъекты в России, включая гражданские аэропорты, Газпром, РЖД, водоканалы, лаборатории, фабрики и заводы, в том числе относящиеся к оборонной, авиационной, химической, металлургической и другим видам промышленности, не говоря уже о рядовых пользователях компьютерной техники, *работают на иностранном программном обеспечении и оборудовании*. В результате вероятный противник с помощью всевозможных «спящих» вредоносных программ и созданных в этом оборудовании преднамеренных уязвимостей получает возможность контролировать нас изнутри и при случае делать с нами все что угодно.

Поэтому весьма серьезную проблему в рассматриваемом плане представляет отсутствие на сегодняшний день *отечественных* предприятий, которые на *отечественной* элементной базе выпускали бы *отечественные* процессоры, контроллеры и прочие компоненты[1]. По словам известного IT-эксперта, одного из разработчиков отечественной операционной системы А. Смирнова, если мы хотим избавиться от технологической зависимости в данной сфере, необходимы значительные вложения, чтобы создать *новую отрасль промышленности, целую новую индустрию*[2].

---

[1] *Чуйков А.* Россия: отстать навсегда? // Аргументы недели. 2019. 17 июля. № 27 (671). С. 8–9.

[2] *Васильченко С.* Россия проигрывает Третью мировую войну: технологическое отставание стало критическим. Почему страна стала аутсайдером в IT-конкуренции // MK.RU. 2019. 19 авг. URL: https://www.mk.ru/politics/2019/08/19/rossiya-proigryvaet-tretyu-mirovuyu-voynu-tekhnologicheskoe-otstavanie-stalo-kriticheskim.html (дата обращения: 23.02.2021).

В связи с этим одним из главных направлений усиления безопасности компьютерных сетей является *активное импортозамещение*. Специалисты заговорили об этом уже давно. Как известно, еще в 2013 г. Президентом РФ был издан Указ от 15 января 2013 г. № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации»[1] (ГосСОПКА). Из находящихся в открытом доступе материалов известно, что полномочия по созданию системы, которая должна обеспечивать безопасность информационной инфраструктуры как в самой России, так и в дипломатических представительствах Российской Федерации за рубежом, этим Указом возложены на ФСБ России. Ее специалистами создана и развивается новейшая информационная система, предназначенная для «обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы страны». Органами ФСБ России разработана также методика обнаружения компьютерных атак и определен порядок обмена информацией между федеральными органами власти в случае их возникновения.

Спустя непродолжительное время после этого в Вооруженных Силах РФ появились войска информационных технологий, о чем 22 февраля 2017 г. официально заявил министр обороны России С.К. Шойгу[2].

Следует напомнить, что задачи по переходу на отечественный софт и защите информационной инфраструктуры закреплены в двух федеральных проектах национальной программы «Цифровая экономика» — «Информационная инфраструктура» и «Информационная безопасность». В утвержденном перечне поручений по итогам «Прямой линии» с главой государства, состоявшейся 20 июня 2019 г., Президент России В.В. Путин поручил Правительству представить предложения по обеспечению технологической независимости и безопасности КИИ России за счет использования преимущественно отечественного программного обеспечения. Исполнить поручение главы государства Правительство должно было к 1 октября 2019 г.[3], и многое в этом направлении

---

1 Российская газета. 2013. 18 янв.

2 В российской армии официально созданы кибервойска // Вести.RU. URL: http://www.vesti.ru/doc.html?id=2858596 (дата обращения: 24.02.2021).

3 Критическую информационную инфраструктуру защитят отечественным ПО // Концорциум Кодекс. 2019. 4 июля. URL: https://kodeks.ru/news/read/kriticheskuu-informacionnuu-infrastrukturu-zaschityat-otechestvennym-po (дата обращения: 18.03.2021).

было сделано. Продолжением этого процесса явилась подготовка проекта Указа Президента РФ «О мерах экономического характера по обеспечению технологической независимости и безопасности объектов критической информационной инфраструктуры»[1], где отмечается, что к 2025 г. объекты КИИ РФ переведут преимущественно на отечественное оборудование. Согласно этому документу Правительству необходимо утвердить требования к программному обеспечению и оборудованию, используемому на объектах КИИ, и порядок перехода на российский софт и оборудование. Под «преимущественным» понимается приоритетное использование российского ПО и (или) оборудования при наличии соответствующих российских аналогов[2]. Однако, по мнению руководителей некоторых хозяйствующих субъектов, такой переход в материальном плане является весьма затратным и не может быть осуществлен в установленные сроки[3].

Поэтому, как отмечают некоторые специалисты, на переходный период для защиты российской КИИ можно обойтись относительно дешевым, но весьма эффективным способом — широким применением технологий, разработанных, испытанных и внедренных еще в конце 1990-х — начале нулевых годов в Санкт-Петербургском Государственном научном центре РФ «Центральный научно-исследовательский и опытно-конструкторский институт робототехники и технической кибернетики». Они связаны с созданием защитных программ-невидимок, реализованных в микропроцессорах (так называемый «компьютерный стелс»). В основе этой системы — защита не отдельных приложений или сервисов, например электронной почты или веб-приложений, а инфраструктуры обмена информацией в целом. Сами средства защиты должны быть неуязвимы для нападения, как, например, известные «межсетевые экраны» (невидимые «сетевые агенты»). Они не имеют ни физических, ни логических (IP) адресов и надежно защищают от любых проникновений. Самое главное, что для их успешной работы не надо менять

---

1 СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=PNPA&n=64055#jy3BUgSLa2k5YD79 (дата обращения: 20.08.2021).

2 Объекты критической информинфраструктуры переведут на российское оборудование к 2025 году // ТАСС. 2020. 29 окт. URL: https://tass.ru/ekonomika/9851951 (дата обращения: 18.03.2021).

3 *Подобедова Л., Сидоркова И., Галимова Н.* Глава «Газпрома» оценил в ₽180 млрд переход компании на российское ПО // РБК. 2021. 23 марта. URL: https://www.rbc.ru/business/23/03/2021/605887c89a79476b5398b6ab?utm_source=yxnews&utm_medium=desktop (дата обращения: 23.03.2021).

«железо» и даже придумывать свою операционную систему. «Сетевые агенты» — по сути, микропрограммы, не видимые никому. Они сами управляют потоками команд и информацией, оставаясь невидимыми и недоступными противнику.

Данные технологии могут и должны быть положены в основу российской глубокоэшелонированной системы защиты, включая частные приложения, операционные системы, облачные структуры и телекоммуникационные каналы связи. В этом плане можно наладить кооперацию с другими заинтересованными странами, например Китаем и Индией[1].

В условиях обострения межгосударственных отношений, разрушения системы однополярного мира, возвращения на мировую арену России и появления новой сверхдержавы — Китая кибероружие становится действенным инструментом глобального противостояния. От того, кто быстрее сможет освоить передовые цифровые технологии, создать мощную систему защиты от государственного кибертерроризма, зависит не только национальная безопасность той или иной страны, но и в целом мировой порядок.

Кроме того, само по себе применение кибероружия в силу колоссального разрушительного потенциала последнего необходимо поставить под международный контроль и приравнять его к использованию иных видов оружия массового поражения.

---

[1] *Угланов А.* Кто парализовал Москву 10 марта? // Аргументы недели. 2021. № 10. С. 1, 8, 9.

Е.С. Ларина, В.С. Овчинский

Координация деятельности спецслужб в киберзащите государства: опыт Израиля

Современные войны все больше переходят в киберпространство. Самый острый узел киберпротиворечий на сегодняшний день представляет собой Израиль с его инновационными и хорошо финансируемыми технологиями и активным военно-разведывательным аппаратом. Он является одним из самых передовых игроков в области кибербезопасности и киберзащиты в мире. Геополитическое положение побудило его разработать и использовать свои современные разведывательные и наступательные возможности для поддержки обычных военных операций. Это стремление к безопасности также привело к участию в процессах построения международных норм для киберпространства.

Активное участие Израиля в кибервойнах уже давно не является ни для кого секретом. Не вызывает также сомнений, что именно Израиль стоял за атакой на Иран вирусов Stuxnet, Duku и Flame несколько лет назад. Специалисты в этой области указывают на Израиль или партнерство между Израилем и США.

В крупной кибератаке в мае 2020 г. на иранский порт Бендер-Аббас тоже обвиняли Израиль, который пытался объяснить свои действия якобы использованием Ираном этого порта в военных целях для помощи террористам в других частях Ближнего Востока, включая Хамас и «Хезболлу». Атака привела к обрушению компьютеров, отслеживающих движение судов и грузовиков в порту, расположенном в стратегическом районе Ормузского пролива в Персидском заливе.

Израиль имеет отношение к кибератаке в мае 2020 г. на расположенный в иранском городе Бендер-Аббас (провинция Хормозган) порт Шахид-Раджаи. Такое утверждение содержится в материале, который опубликовала газета «The Washington Post», ссылающаяся на источники. Работа порта в тот день была нарушена в связи с тем, что регулирующие судоходство компьютеры неожиданно вышли из строя. На следующий день иранские власти сообщили, что причиной этого была кибератака.

Обратная реакция не заставляет себя ждать. Представители разведки и служб, занимающихся вопросами кибербезопасности, полагают, что атака стала ответом на предпринятую в апреле 2020 г. неудачную попытку взломать компьютеры, отвечающие за водораспределительные системы в сельской местности в Израиле.

В 2020 г. группа иранских хакеров *Pay2Key*, целенаправленно действующих против Израиля, в своем аккаунте в твиттере заявила о взломе компьютеров нескольких компаний, в том числе ведущего израильского концерна ВПК «Таасия авирит» («Авиационная промышленность Израиля»). Стало известно, что также взломаны серверы его дочерней компании «Альта». Взломщики опубликовали личные данные более тысячи сотрудников компании, включая высокопоставленных представителей отдела по обеспечению кибербезопасности. *Pay2Key* заявила, что захватила почти 1 терабайт данных, включающих, в частности, массив крупной израильской оборонной компании «Elbit».

В декабре 2020 г. хакерской атаке подверглись серверы и компьютеры страховой компании «Ширбит». В открытый доступ были выложены данные клиентов «Ширбит», включая копии внутренних паспортов («теудат зеут»). Ранее компания выиграла тендер на страхование государственных служащих, в том числе сотрудников силовых структур. Ответственность за эту атаку взяли на себя хакеры международной группы *Black Shadow*.

В 2020 г. израильская полиция открыла 8377 кибердел. Часть из них связаны с кражей личных данных и фальсификацией документов. При этом всего 350 дел были открыты по самым популярным в мире случаям кражи кредитных карт.

В 2021 г. бывший премьер Б. Нетаньяху публично раскрыл главную миссию Моссада, заявив, что первостепенная задача спецслужбы — помешать Ирану обзавестись собственным ядерным оружием.

Атаки на ядерные объекты и убийства иранских ученых — операции, проводившиеся Моссадом в прошлом, вполне вероятно, будут проводиться и в будущем.

В такой напряженной обстановке роль кибероружия в борьбе Израиля с Хамасом и Ираном становится одним из главных методов военного и психологического воздействия. Израиль становится мировым полигоном обкатки реальных боевых действий. Поэтому так важно изучить национальную политику кибербезопасности Израиля, сделать обзор его национальной организационной структуры, рассмотреть ключевые стратегические документы,

а также изучить основные международные и национальные партнерства.

В конце 2020 г. Центром исследований безопасности (Zürich) был опубликован отчет «Национальная кибербезопасность и позиция киберзащиты Израиля». В этом отчете содержится краткий обзор национальной политики кибербезопасности и киберзащиты Израиля, показаны ключевые события, которые повлияли на восприятие Израилем угрозы, и излагаются эволюция и сдвиги в политике кибербезопасности и обороны Израиля.

В Израиле принят комплексный подход к политике кибербезопасности, в котором особое внимание уделяется повышению кибернадежности и киберустойчивости. Это делается в тесной координации с национальными и международными, государственными и частными заинтересованными сторонами. Кибербезопасность рассматривается как ключевой потенциал для экономики и инноваций Израиля.

Активная киберзащита и оборонительные операции являются двумя столпами израильской стратегии кибербезопасности 2017 г. Подход Сил обороны Израиля определяется четырьмя доктринальными принципами Бен-Гуриона: сдерживание, решающая победа, раннее предупреждение и союзы.

Стратегическая политика кибербезопасности Израиля возглавляется и координируется на высшем уровне Национальным управлением кибербезопасности Израиля (INCD), которое находится под непосредственным руководством премьер-министра и его офиса. INCD выполняет задачи бывшего Национального управления кибербезопасности (NCSA), имевшего оперативную ориентацию и более ориентированного на политику Национального управления кибербезопасности Израиля (INCB). На оперативном уровне усилия распределяются по проблемным областям между Моссадом, Шин-Бетом, полицией Израиля и INCD. На практике эти агентства демонстрировали различия в основных ценностях и операционных подходах, которые вызвали недоразумения INCD.

Основными органами киберзащиты Сил обороны Израиля (IDF) являются их Подразделение 8200 (для наступательных кибероперациий) и Управление C4I (для оборонительных операций и безопасности инфраструктуры). Шин-Бет, Моссад, полиция Израиля и министерство юстиции обладают компетенцией киберзащиты. Они сотрудничают и координируются INCD.

Правительство Израиля активно привлекает к партнерству в области киберзащиты академические круги и частный сектор,

например к совершенствованию своих НИОКР. Его крупнейшее партнерство — инновационный парк *CyberSpark*.

Защита критически важной инфраструктуры (CIP) была основной мотивацией первых усилий Израиля по обеспечению кибербезопасности гражданского населения. Подобные решения сначала были достигнуты на краткосрочной, прагматической и специальной основе. Это привело к относительной децентрализации системы. Однако за последние пару лет израильское правительство приложило значительные усилия для объединения различных гражданских агентств по кибербезопасности в одну организацию — Израильское национальное управление кибербезопасности (INCD).

INCD является частью канцелярии премьер-министра Израиля. Только три других агентства — Шин-Бет, Моссад и Израильский комитет по атомной энергии — напрямую подчиняются канцелярии премьер-министра (PMO). Это показывает, насколько важным считается INCD для безопасности Израиля. Задача INCD — организовать ландшафт гражданской кибербезопасности. Таким образом, INCD координирует все аспекты гражданской киберзащиты, начиная от оперативной защиты и заканчивая наращиванием технологического потенциала и политическими предложениями. Некоторые задачи гражданской кибербезопасности остаются за пределами компетенции INCD, например, те функции, которые требуют участия израильской полиции или разведывательных служб.

Наблюдается явная тенденция к централизации ранее децентрализованного ландшафта гражданской кибербезопасности. Гражданская кибербезопасность дополняется военной киберзащитой, которая находится под эгидой Сил обороны Израиля (ЦАХАЛ). Тем не менее организационное руководство может смещаться. В мирное время INCD отвечает за гражданские кампании национальной обороны, в то время как ЦАХАЛ возглавляет наступательные и оборонительные кампании на национальном уровне в чрезвычайных ситуациях или во время войны.

Ключевые национальные тенденции

Израиль — региональная держава с процветающей экономикой, которая с момента образования сталкивается с серьезными угрозами своей национальной безопасности. В последние десятилетия он демонстрирует готовность проецировать силу посредством военных операций и вмешательства в соседние войны. Сегодня Израиль считает себя одним из пяти самых могущественных государств с точки зрения киберпространства. Это восприятие опирается на два столпа: (1) сильные и активные военные и надежные

разведывательные службы, а также (2) инновационный гражданский сектор.

Что касается первого, то IDF использует свои кибервозможности для сложных кибератак (например, Stuxnet, 2017) или шпионских кампаний (например, Flame и Duqu, 2011–2012). Между тем внутреннее разведывательное сообщество (Шин-Бет и Моссад) интегрирует кибернетику в свой подход к укреплению внутренней безопасности, участвуя в важных процессах обмена информацией с различными правительственными органами. Разведка и наступательные киберспособности также применяются для поддержки обычного военного сектора. Этот проактивный подход к защите Государства Израиль и его суверенитета прослеживается на протяжении всей военной истории Израиля и изложен в его текущей стратегии обороны ЦАХАЛа.

В рамках давнего стратегического партнерства с США Израиль поддерживает тесные связи с американскими агентствами по киберзащите. Однако несмотря на то, что Израиль считается основным стратегическим партнером НАТО, имеет хорошие отношения с Россией, укрепляет связи с Индией и в прошлом имел военное сотрудничество с Великобританией и Францией во время Суэцкого кризиса, у него нет официальных союзников с серьезными обязательствами. В результате Израиль стремится создать мощный военный потенциал для сдерживания своих противников. Вдобавок к этому и обязательная военная служба, и стремление ЦАХАЛа к технологическому превосходству сыграли важную роль в формировании развития киберпотенциалов Израиля. Что касается последнего, то в гражданский киберпотенциал были вложены значительные инвестиции.

Несмотря на то, что экономика Израиля сталкивается с различными трудностями, в глобальном масштабе она по-прежнему занимает 31-е место по уровню ВВП на душу населения (2019 г.). Он тратит от 6 до 8% своего ВВП на оборону (2015 г.), также занимает первое место в мире по внутренним расходам на исследования и разработки по отношению к ВВП (более 4,5% ВВП в 2019 г.). Этот акцент на исследованиях и разработках, а также стимулирующая роль технических подразделений ЦАХАЛа (например, Подразделение 8200) обеспечивает благоприятную среду для процветания стартапов в секторе высоких технологий.

На долю 420 израильских компаний, занимающихся кибербезопасностью, приходится примерно 20% мировых инвестиций в кибербезопасность (815 млн долл. США), экспорт которых составляет

3,8 млрд долл. США (2018 г.), или 8% мирового рынка решений для кибербезопасности (2017 г.).

Что касается международных усилий, Израиль был членом пятой Группы правительственных экспертов Организации Объединенных Наций (ГПЭ ООН) в области информации и телекоммуникаций и Женевского диалога об ответственном поведении в киберпространстве и тем самым участвовал в установлении норм приемлемого поведения в киберпространстве. Израиль также подписал Конвенцию Совета Европы о киберпреступности (2019 г.) и установил двусторонние отношения сотрудничества (например, с США в 2016 г., Болгарией в 2018 г. и Австралией в 2017 г.).

Возможно, это удивительно, но у государства с такой надежной национальной оборонной политикой нет официальной стратегии национальной безопасности. Фактически, руководство Израиля избегает публикации каких-либо декларативных документов. Действительно, прошлые попытки сформулировать стратегию национальной безопасности не увенчались успехом из-за значительных политических и бюрократических препятствий. Вместо того чтобы полагаться на формализованные процессы планирования, усилия Израиля по обеспечению безопасности чаще осуществляются на разовой основе. Наиболее важные стратегии и программные документы описаны ниже.

Доктринальные принципы Израиля Д. Бен-Гуриона 1953 г. Несмотря на то, что основные доктринальные принципы политики безопасности Израиля не формализованы в официальных публикациях, они хорошо известны. В прошлом премьер-министр Давид Бен-Гурион представил их в своем докладе Кабинету министров от 18 октября 1953 г. С тех пор израильский политический и оборонный истеблишмент динамично адаптировал эти принципы.

Эта великая стратегия — Tfisat HaBitachon — была задумана более 65 лет назад в другом контексте безопасности: молодая нация была измучена израильско-арабской войной и находилась под угрозой вторжения со стороны своих арабских соседей. Тем не менее эти доктринальные принципы ближе всего к формальной стратегии национальной безопасности. Эти принципы и призыв Бен-Гуриона 1948 г. к Израилю поддерживать «последовательную и эффективную готовность к обороне в любое время» даже после окончания боевых действий по-прежнему актуальны для сегодняшних стратегий кибербезопасности и киберзащиты.

Обобщая эти принципы, Бен-Гурион приказал израильским военным приложить усилия:

— к защите государства, его жителей, инфраструктуры и интересов;

— сдерживанию потенциальных атак;

— формированию союзов с великими державами;

— развитию сложных средств раннего предупреждения, чтобы компенсировать отсутствие у Израиля стратегической глубины;

— достижению технологического превосходства и качественного преимущества, чтобы компенсировать нехватку у Израиля критических ресурсов;

— обеспечению быстрой и решительной победы в случае противостояния.

Стратегия Эйзенкота 2015 г. В 2015 г. ЦАХАЛ под руководством бывшего начальника Генштаба Гади Эйзенкота опубликовал «первую доктрину общественной защиты», которая включала, среди прочего, взгляд на использование кибервозможностей. В частности, эта стратегия признает развитие киберпотенциала противником, а также киберсферы как одну из четырех соответствующих областей обороны Израиля (наряду с сушей, морем и воздухом). Стратегия также рассматривает киберпотенциал как интегрированную поддержку обычной обороны и наступления на всех уровнях боя (т.е. стратегическом, оперативном и тактическом). ЦАХАЛ считает военную киберзащиту и наступление жизненно важными для обеспечения: функционирования государства и институтов ЦАХАЛа, использования разведывательных данных, коллективной защиты, операций влияния и достижения легитимности, а также правовых ответных мер. Наконец, эта стратегия подчеркивает стратегическое и тактическое сдерживание посредством кибервойны.

Национальная стратегия кибербезопасности Израиля 2017 г. До 2017 г. Израиль никогда не формулировал всеобъемлющую официальную национальную стратегию кибербезопасности. Стратегия INCD является первым официальным документом по национальной безопасности Израиля после декларации Бен-Гуриона 1953 г. о стратегических принципах. Этот краткий документ описывает приоритеты INCD. Помимо общих целей — например, защитить экономическую и социальную мощь Израиля — она не имеет непосредственного отношения к стратегии ЦАХАЛа Эйзенкота 2015 г. В частности, в ней описывается, как Израиль планирует улучшить свою киберустойчивость, системную устойчивость, гражданскую национальную киберзащиту, а также излагаются основы создания и задачи NCSA. Наконец, она также касается наращивания потенциала и международного сотрудничества.

Национальная стратегия кибербезопасности: сферы, задачи и приоритеты

Национальная стратегия кибербезопасности (2017 г.) — первая всеобъемлющая официальная киберстратегия Израиля. Она включает как прямые действия государства по противодействию киберрискам, так и косвенные усилия, направленные на поддержку и сотрудничество с частным сектором.

Эта всеобъемлющая стратегия знаменует собой отход от ранее принятых политических решений, которые были сосредоточены на решении насущных проблем, а не на видении более широкой картины.

Концепция операций

Первая часть Национальной стратегии кибербезопасности относится к гражданской деятельности по киберзащите и состоит из трех уровней:

1. ***Повышение «совокупной киберустойчивости» к повседневным угрозам***. Это позволяет превентивно снижать риски. Как указано в Постановлении Правительства № 2443 2015 г., государство продвигает усилия по обеспечению безопасности, предпринимаемые частным сектором, например, создавая стимулы, правила, внедряя передовую практику. Правила в основном применяются в отношении предложения киберпродуктов и услуг; INCD устанавливает обязательные стандарты для основных секторов и критической инфраструктуры. Что касается спроса, оно спонсирует повышение осведомленности и продвижение знаний в частном секторе.

2. ***Развитие «системной киберустойчивости» главным образом за счет улучшения межправительственного и международного сотрудничества, а также реагирования на инциденты***. Системная киберустойчивость зависит от событий и является реактивной, независимо от конкретных событий. Общие усилия заключаются в сборе и обмене разведывательной информацией секторальными центрами, создании механизмов раннего предупреждения, возможностей реагирования на инциденты и центров обработки вызовов. CERT-IL (Израильская группа реагирования на компьютерные чрезвычайные ситуации) координирует системные усилия по обеспечению киберустойчивости путем сотрудничества с частным сектором через отраслевые киберцентры, а также путем прямой поддержки компаний, подверженных риску, и сотрудничества на местном и глобальном уровнях.

3. ***Усиление гражданской «национальной киберзащиты» для смягчения наиболее опасных киберугроз национальной без-***

опасности. Третий уровень основан на двух предыдущих уровнях и включает не только защитные меры (например, защитные операции CERT-IL и оценку ситуации), но также активную киберзащиту и наступательные действия органов национальной безопасности и правоохранительных органов в целях противодействия как государственным, так и негосударственным организациям для достижения сдерживания агрессии.

Первый уровень — это проблема, которую организациям необходимо решить самостоятельно, без существенной помощи со стороны государства. И чем выше уровень угрозы, тем больше объем ответственности, которая передается от частного сектора к правительству. Третий уровень — исключительная задача государственных органов.

Во второй части Национальной стратегии кибербезопасности описываются образовательные и производственные усилия по наращиванию потенциала, которые закладывают основу для кибероперациий. В ней описываются планы по улучшению национальной киберэкосистемы: стимулирование государственных производств и коммерческих НИОКР, академических исследований и образования от первого класса до университета, а также поддержка разработки перспективных технологий двойного назначения, которые могут использоваться государством.

В третьей части подробно описываются конфигурация и полномочия INCD, которое контролирует реализацию концепций, изложенных в первых двух частях, и объединяет ответственные учреждения для всех трех уровней (т.е. надежности, устойчивости и защиты). INCD также отвечает за международную координацию и формулирование правовых рамок для киберпроблем. Оно также координирует национальные усилия по киберзащите с военными и службами безопасности. Между тем ЦАХАЛ объединяет наступательные и оборонительные кампании в случае возникновения чрезвычайной ситуации.

Общедоступного плана реализации Национальной стратегии кибербезопасности 2017 г. нет. Однако различные проекты INCD конкретизируют некоторые его аспекты. Сюда входят такие проекты, как «Высокий замок», «Хрустальный шар», «Витрина» и «Кибернет+». Они направлены на повышение способности Израиля обнаруживать и предотвращать киберинциденты, улучшать координацию и разведку, повышать готовность и управление рисками, а также способствовать обмену данными и процессами распределения между учреждениями.

«Высокий замок», например, является платформой для государственных и частных заинтересованных сторон, позволяющей улучшить возможности обнаружения, расследования и блокировки. «Хрустальный шар» сочетает в себе различные инструменты сбора информации об угрозах, уточняет результаты исследования. «Высокий замок» создает единую проекцию угроз в целях улучшения возможностей анализа ситуации для разведывательных служб и гражданских заинтересованных сторон. «Витрина» оценивает подверженность рискам и степень готовности критически важной инфраструктуры. Наконец, «CyberNet+» — это платформа обмена информацией о государственно-частном партнерстве, которая позволяет анонимно сообщать об угрозах. Эти проекты не представляют собой комплексную стратегию, но предназначены для решения некоторых из наиболее острых проблем кибербезопасности, с которыми сталкивается Израиль.

Национальная стратегия киберзащиты

Несмотря на то, что ЦАХАЛ считается одной из наиболее «способных в киберпространстве» армий, у Израиля нет специальной и публичной стратегий киберзащиты. Однако в гражданской — Национальной стратегии кибербезопасности от 2017 г. излагаются оборонительные и наступательные возможности ЦАХАЛа. Он также выступает за гибкое руководство и контроль между IDF и INCD.

Несмотря на отсутствие плана реализации, известно, что стратегические цели реализуются как минимум двумя организациями, а именно C4I Directorate (для киберзащиты) и Unit 8200 (для киберпреступлений). В стратегии IDF 2015 г. не рассматривается киберзащита, но в ней говорится, что кибернетика выполняет вспомогательную функцию для операций IDF.

Кроме того, IDF в своей стратегии киберзащиты применяет как минимум четыре доктринальных принципа Бен-Гуриона:

1. В киберпространстве довольно сложно добиться сдерживания. Для реализации плана Бен-Гуриона по удержанию врагов Израиля от нападения Ури Тор (2017 г.) ввел концепцию «кумулятивного сдерживания». Согласно этому подходу, который широко применяется в обычных подразделениях ЦАХАЛа, сдерживание необходимо «подпитывать» спорадическими вспышками насилия в ответ на агрессию. Армия обороны Израиля создала прецедент, когда в режиме реального времени отреагировала на кибератаку, взорвав кибер-штаб-квартиру Хамаса, тем самым предоставив «возможность увидеть будущее войны» (2019 г.).

2. Решающая победа принесла ограниченный успех. Несмотря на то, что израильское Подразделение 8200 проводило различные изощренные кибератаки, ни одна из них сама по себе не привела к решающей победе. Вместо этого они поддерживают сбор разведданных (например, с помощью Flame) или саботаж (например, с помощью Stuxnet).

3. Раннее предупреждение оказалось успешным благодаря средствам киберпространства. Действительно, Подразделение 8200 обеспечило несколько ранних предупреждений, которые помогли предотвратить внутренние террористические атаки и предсказать иностранную агрессию. Остаются некоторые сомнения относительно возможностей обнаружения и предупреждения изощренных кибератак.

4. Альянсы не обсуждаются в общедоступных документах. Однако предполагается, что между IDF и киберагентствами США налажено определенное международное сотрудничество, особенно во время разработки Stuxnet.

Ключевые принципы киберполитики

Концепция кибербезопасности в Израиле становится все более целостной с момента введения режима кибербезопасности в 1998 г. Как и в других развитых странах, в начале 2000-х гг. первоначальный акцент в области гражданской кибербезопасности сместился с CIP на техническое превосходство. В 2015 г. упор был сделан на реорганизацию задач разведывательного сообщества и гражданского сектора и создание правовой базы. Постановления правительства от 2017 г. были самыми последними усилиями по централизации и сокращению избыточности, в результате чего удалось создать прочную и устойчивую киберэкосистему. В экосистеме правительство приложило значительные усилия для координации правительственных, военных и частных заинтересованных сторон. Однако, несмотря на институциональное разделение военной и гражданской кибербезопасности и киберзащиты, задачи и информация часто неофициально распределяются между организациями и агентствами.

В стратегии Израиля выделяются два момента. Во-первых, военные развивают свои возможности киберзащиты и разведки в ответ на явно упомянутых врагов (Иран, Ливан, Хезболла, Хамас, Сирия, ИГИЛ, Палестинский исламский джихад и т.д.) Немногие государства формируют свою киберзащиту, чтобы противостоять конкретно идентифицированным субъектам угроз. Чтобы противостоять таким угрозам, национальные агентства получают значи-

тельное финансирование, тесно сотрудничают и обмениваются информацией. Это возможно несмотря на то, а может быть, и потому, что официальная стратегия киберзащиты не была опубликована.

Во-вторых, гражданская стратегия кибербезопасности активно вовлекает частный сектор и поддерживает в использовании его опыта, одновременно укрепляя расширяющуюся израильскую высокотехнологичную промышленность. Инвестиции в кибербезопасность рассматриваются как потенциал для экономики и инноваций Израиля.

Инвестиции способствуют накоплению опыта и знаний, которые укрепляют статус Израиля как технологически ориентированной «нации стартапов». Оборотной стороной является то, что распространение опыта в частном и государственном секторах требует большей координации для эффективного вклада в национальную безопасность. Создание INCD является наиболее значительным шагом на пути к совершенствованию экспертных знаний, стабильной правовой базе, централизации полномочий и использованию четких способов коммуникации. INCD, координируя действия с различными участниками, использует опыт как государственного, так и частного сектора для стабилизации и защиты израильского киберпространства.

Текущие общественные структуры кибербезопасности и инициативы

Сотрудничество и направления политики между IDF, INCD, Шин-Бет и другими правительственными министерствами часто засекречены. Поскольку новый киберзакон все еще находится на рассмотрении, официальных направлений политики и сотрудничества нет. Однако отсутствие официальной политики позволяет участникам сотрудничать с определенной степенью гибкости. Например, если CERT-IL обрабатывает случай, когда компьютер представляет угрозу для большего числа сетей, он обычно полагается на сотрудничество компании. Однако если последняя не будет сотрудничать, CERT-IL может относительно свободно сотрудничать с различными учреждениями, например с полицией Израиля или Шин-Бетом, для решения проблемы. Эти службы безопасности могут, в частности, использовать свои полномочия, чтобы заставить компанию подчиниться.

Израильское национальное управление кибербезопасности (INCD) составляет ядро гражданской архитектуры кибербезопасности и является результатом слияния NCSA и INCB в 2018 г. Таким образом, оно подчиняется непосредственно канцелярии

премьер-министра, что позволяет передать вопросы последнему и косвенно подкрепить политическое направление этой должности. Перед INCD стоят следующие задачи:

- планирование стратегической политики для повышения киберустойчивости Израиля к рискам путем поддержки важнейших инфраструктур и введения нормативных правовых актов;
- реализация и регулирование национальной киберстратегии на национальном уровне (повышение надежности, устойчивости и защиты, включая CERT-IL и CIP);
- содействие международному сотрудничеству, а также разработка правовых рамок для кибердеятельности (внутри страны и за рубежом);
- комплексное управление кампаниями национальной обороны (в мирное время);
- повышение устойчивости сотрудничества с израильской полицией и Министерством юстиции;
- поддержка Шин-Бета, ЦАХАЛа, Моссада, израильской полиции и Министерства юстиции в усилении гражданской киберзащиты.

Несмотря на то что на бумаге INCD является центральным и наиболее влиятельным агентством, его сотрудничество с другими агентствами часто затруднено. Что наиболее важно, основные ценности и операционные подходы Шин-Бета и INCD существенно различаются, что приводит к многомесячным войнам за власть, особенно в отношении CIP. Кроме того, хотя разведывательное сообщество фокусируется на защите безопасности Израиля от внутренних угроз с помощью важных технических возможностей, оно часто рассматривает конфиденциальность и законность как второстепенные вопросы. Однако INCD стремится координировать такие усилия в более широком национальном контексте и указывает на необходимость законности. Для INCD опора на технический опыт других агентств (в первую очередь, Шин-Бета, Моссада и Подразделения 8200) может оказаться палкой о двух концах. С одной стороны, вовлекая эти агентства в выполнение своих задач, INCD может перераспределить ресурсы на другие приоритеты, помимо развития технических знаний внутри компании. С другой стороны, оно подвержено внешнему влиянию, особенно со стороны Шин-Бета.

Ожидается рост бюджета и количества сотрудников INCD. В 2019 г. бюджет оценивался в размере от 32 до 64 млн долл. США, т.е. бюджет 2017 г. увеличился вдвое. Кроме того, прогнозирова-

лось, что штат сотрудников вырастет с 220 в 2017 г. до 250 человек в 2019 г.

Наиболее сложной проблемой, с которой столкнется INCD в будущем, является нечеткая правовая база — в настоящее время она пересматривается, но прослеживается тупик в законодательной сфере. В настоящем виде INCD позволяет премьер-министру заказывать исчерпывающее расследование и наблюдение за кем угодно — даже политическими противниками — практически без надзорных механизмов.

Шин-Бет и Моссад действуют бок о бок с израильскими правоохранительными органами и гражданскими службами кибербезопасности. Они обмениваются опытом и информацией, но остаются отделенными от INCD в силу своего мандата в качестве разведывательных служб. Вот почему нет общедоступной информации об их задачах, действиях, оперативных возможностях и сотрудничестве с другими агентствами, связанными с кибербезопасностью.

Шин-Бет также участвует в киберзащите, но с другими обязанностями, нежели ЦАХАЛ. Он участвует в защите критически важной инфраструктуры связи. Его задача киберзащиты является относительно всеобъемлющей, примером чего может служить взлом Ираном (предположительно) мобильного телефона теперь уже альтернативного премьер-министра Бенни Ганца в 2018 г. Сообщество безопасности было обеспокоено тем, что Иран вмешается в выборы 2019 г. В обязанности Шин-Бета входило снижение этого риска.

Полиция Израиля. Приблизительно 20 человек работают в отделе киберпреступности — LAHAV 433 — полиции Израиля, это самый слабый субъект израильского сообщества безопасности. Он не оказывает существенного влияния на разработку политики.

Национальные структуры и инициативы по киберзащите: организация, полномочия, правовые аспекты и операционные возможности

Различные учреждения помогают создать надежную киберзащиту (третий уровень израильской стратегии кибербезопасности). Многие из них имеют перекрывающиеся области ответственности. В числе основных можно выделить Подразделение 8200 ЦАХАЛа и управление C4I, Шин-Бет, INCD и Моссад, а также — в меньшей степени — израильскую полицию и Министерство юстиции. Два подразделения ЦАХАЛа, упомянутые первыми, являются наиболее важными для киберзащиты Израиля и будут рассмотрены более подробно.

Подразделение 8200, также известное как центральное подразделение сбора разведывательных данных или израильское национальное подразделение SIGINT (ISNU), охватывает наступательный спектр военного использования кибервозможностей. Оно подчиняется Управлению военной разведки (AMAN).

После того как «Пламя» стало достоянием гласности в 2012 г., ЦАХАЛ признал, что Подразделение 8200 проводит наступательные кибероперации. Помимо «Пламени» Подразделение 8200 якобы разработало Duqu (2012), а также Stuxnet в сотрудничестве с Агентством национальной безопасности США. Эти операции выявили аспекты его мандата: саботаж промышленных объектов, шпионаж и поддержка традиционных вооруженных сил.

Подразделение придает большое значение оперативной гибкости: его правовые ограничения относительно слабые, организационная культура допускает или поощряет беспрецедентные наступательные действия и оно оперирует значительными финансовыми ресурсами. Подразделение имеет достаточно мощные оперативные возможности, а также тесные связи со своим американским коллегой АНБ. Разведка, не входящая в состав IDF (Моссад и Шин-Бет), сотрудничает с Подразделением 8200. В Израиле, по некоторым оценкам, 90% всех разведывательных материалов собирается Подразделением 8200, что приводит к участию во всех основных операциях Моссада.

Солдаты присоединяются к Подразделению в 18 лет и покидают его через четыре года, создавая проблемы для обучения новобранцев и ежегодно заменяя 20% личного состава. По некоторым оценкам, к Подразделению 8200 приписано 5000 солдат (2016 г.).

Кроме того, следует объяснить влияние Подразделения 8200 на технологическую отрасль Израиля. Перед тем как поступить в подразделение в возрасте 17 лет, перспективные ученики отбираются на основе их аналитических способностей. Они служат четыре года, начиная с 18-летнего возраста. В течение этого времени на них возлагается высокая ответственность, от них требуют проявления творческого подхода. По некоторым данным, это повышает шансы выпускников Подразделения 8200 запускать успешные стартапы или преуспевать в солидных компаниях. Благодаря обязательному резерву до достижения 50-летнего возраста IDF может рассчитывать на опытных технических экспертов, которые в случае необходимости будут в распоряжении ЦАХАЛа.

Задача ***Управления C4I***, также известного как Корпус C4I или Корпус телепроцессов, заключается в защите инфраструктуры связи и систем телепроцессов ЦАХАЛа.

Организационно Управление C4I подчиняется Управлению компьютерных услуг (также известному как Atak). В последнее время подход C4I к киберзащите сместился в сторону «активной защиты», которая предполагает возможность сдерживающих и упреждающих атак. Это развитие соответствует доктринальным принципам государственной обороны Бен-Гуриона 1953 г., особенно призыву к быстрой и решительной победе, сдерживанию, качественному превосходству и высочайшим возможностям раннего предупреждения. Управление C4I создало центр, который объединяет как компьютерное подразделение, так и силы военной разведки. Однако он сталкивается с финансовыми ограничениями, что привело к сокращению его руководства с четырех до трех бригадных генералов.

Ключевая общественная организационная структура

Одним из основных преимуществ израильской организационной структуры является то, что она становится тесной и хорошо связанной экосистемой кибербезопасности, где может происходить быстрый, эффективный и неформальный обмен информацией. Действительно, поскольку большинство киберэкспертов начинают свою карьеру в качестве солдат в Подразделении 8200, они, как правило, поддерживают социальную сеть, которая создает прочные связи между частным и государственным сектором, военными и разведывательным сообществом.

В более общем плане структуры кибербезопасности и киберзащиты Израиля становятся все более централизованными в рамках IDF и INCD. Такая централизация дает определенные преимущества: консолидация опыта и улучшенный обмен информацией. Однако консолидация власти в канцелярии премьер-министра в сочетании с общественным признанием нарушения конфиденциальности в обмен на усиление общей безопасности, а также разделение Кнессета может привести к злоупотреблениям политической и кибервластью, антидемократическим действиям и нарушениям прав человека (например, этнически дискриминационное наблюдение исключительно за палестинскими гражданами или политическими противниками). Текущий законопроект ***о киберзащите и национальном киберуправлении*** является хорошим примером тенденций отсутствия системы сдержек и противовесов. Согласно указанному проекту INCD будет разрешено конфисковывать оборудование, связанное с кибератакой, даже без постановления суда. INCD также может отслеживать весь интернет-трафик.

Кроме того, центральное положение INCD в канцелярии премьер-министра следует рассматривать в контексте исторически и технически мощных, конкурентоспособных разведывательных служб. Соответственно, можно наблюдать три тенденции.

Во-первых, INCD призвано решить проблему межведомственной борьбы. Действительно, объединяя технический опыт — через CERT-IL, а также будучи стратегическим лидером в разработке структуры кибербезопасности Израиля, INCD должно стать неоспоримым кибер-авторитетом в Израиле. Тем не менее возникают опасения по поводу влияния других организаций, особенно Шин-Бета.

Во-вторых, INCD соответствует пониманию комплексного характера киберпроблем в министерствах. Размещаясь в канцелярии премьер-министра, оно не входит в состав какого-то конкретного министерства и, таким образом, генерирует опыт, ответственность и полномочия для определения повестки дня по кибервопросам только для этого министерства.

В-третьих, позиция INCD также указывает на высокую степень приоритетности кибербезопасности и киберзащиты. Для правительства Израиля борьба с киберугрозами является одним из важнейших приоритетов национальной политики и безопасности — как для военной, так и для гражданской сферы.

В 2015 г. бывший в то время начальником штаба Гади Эйзенкот объявил об объединении всех киберэлементов в единое целое — аналогично киберкомандованию США. Несмотря на то, что Эйзенкот выступал за реорганизацию, реализация этих планов была отложена, а существующее организационное разделение между Управлением C4I, спецслужбами и Подразделением 8200 сохраняется (2018 г.). На фоне этих реорганизаций останется одна организационная концепция: ЦАХАЛ будет поддерживать небольшие изолированные киберподразделения, солдаты которых действуют по принципу служебной необходимости, чтобы облегчить выявление утечек.

Еще одно средство приспособления израильской киберзащиты к нестабильной ситуации на Ближнем Востоке — это ее гибкая организационная адаптируемость при повышении уровня угрозы. В мирное время INCD отвечает за управление национальной киберзащитой. Во время чрезвычайных ситуаций ЦАХАЛ координирует наступательные и защитные киберкампании на национальном уровне. Планы IDF по созданию единого киберкомандования на 2015–2017 гг. показывают, что оно все еще находится в фазе трансформации в отношении киберпроблем.

В частности, киберзащита (Управление C4I) работает в наступательном направлении, но остается отделенной от военной разведки (Подразделение 8200). Споры о концептуализации и организации киберзащиты ЦАХАЛа продолжатся и в будущем. Наиболее актуальными будут вопросы унифицированного киберпотенциала, сотрудничества с гражданскими агентствами и перспективы использования кибервозможностей в военных целях (в поддержку традиционных сил или отдельного подразделения, аналогичного воздушному, наземному и морскому).

Недавняя атака иранских хакеров на систему водоснабжения Израиля побудила оборонный концерн «Рафаэль» сформировать консорциум с ведущими компаниями в разных сферах. Цель такого сотрудничества — защита от грядущих атак, сообщает «The Jerusalem Post».

«Израильский киберконсорциум операционных технологий» будет действовать совместно с Национальным кибердиректоратом. Он разработает комплексные технологические решения для защиты от хакеров критически важной инфраструктуры: вода, электроэнергия, транспорт, нефть и газ.

С одной стороны, в консорциум будут входить те организации, которые управляют такой инфраструктурой. Среди них — ТАШАН, обслуживающая крупные нефтехранилища в Хайфе, и Электрическая компания Израиля («Хеврат Хашмаль»). С другой стороны, к сотрудничеству присоединятся компании из сферы кибербезопасности. Вместе они предложат «проверенное в бою комплексное решение» для крупных организаций.

Оценки финансовых ограничений не имеют информативной ценности, поскольку официально публикуемые данные немногочисленны. Например, бюджет INCD постоянно увеличивается, однако неясно, сколько внешних ресурсов используется в рамках сотрудничества с другими агентствами. Нет данных по бюджету Моссада, Шин-Бета, Подразделения 8200 или C4I.

Киберзащита: партнерские структуры и инициативы

Государственно-частное партнерство в сфере киберзащиты. Постановлением правительства № 3611 (2011 г.) INCB (в настоящее время — INCD) предписано «способствовать координации и сотрудничеству между правительственными органами, оборонным сообществом, академическими кругами, промышленными организациями, предприятиями и другими органами, имеющими отношение к киберпространству». Сегодня эти усилия приносят свои плоды: различные платформы для сотрудничества

позволяют распространять знания в разных секторах. Семинар Ювваля Неемана Тель-Авивского университета (основан в 2002 г.) и Междисциплинарный центр кибериссследований имени Блаватника (открыт в 2014 г.) вместе с INCB ознаменовали первое сотрудничество правительства и академических кругов в исследованиях, связанных с киберпространством. Результатом стала платформа для неформального обмена с представителями частного, государственного, академического и военного секторов.

CyberSpark, израильская экосистема киберинноваций в Беэр-Шеве, является наиболее заметным израильским проектом государственно-частного партнерства в области киберзащиты. Военные (например, Управление C4I и Подразделение 8200) и правительство (например, CERT-IL) решили переместить туда важные органы своей киберзащиты. Этот проект привлек и частный сектор. Такие компании, как *Oracle*, *Lockheed Martin*, *IBM*, *Dell*, *Deutsche Telekom* и *PayPal,* решили стать частью этой экосистемы. Несмотря на то, что такие экосистемы не являются официальными государственно-частными партнерствами для киберзащиты, они способствуют укреплению сотрудничества. Наконец, платформа для обмена анонимной информацией (CyberNet+) позволяет IDF сотрудничать с частным сектором, получая прибыль и одновременно важную информацию.

Международное партнерство в области киберзащиты. INCB провело «национальные и международные учения по повышению готовности Государства Израиль в киберпространстве» и продвинуло «сотрудничество в киберпространстве с параллельными организациями за рубежом» (2011 г.). Обнародованы лишь некоторые результаты. Израиль не является союзником НАТО и имеет прочные связи с военными США и киберагентствами, в первую очередь с АНБ. В 2016 г. Израиль и США подписали декларацию о киберзащите, в которой описывается функциональная связь в реальном времени для обоих групп реагирования на компьютерные чрезвычайные ситуации. Еще одно партнерство было зафиксировано в меморандуме о взаимопонимании между США и правительством Израиля по вопросам внутренней безопасности (2008 г.).

На конференции Cyber Week в июне 2019 г. директором INCD был представлен список из 36 стран и 13 организаций и компаний, с которыми Израиль установил международное сотрудничество, но не уточнялось, как они сотрудничают.

Программы повышения осведомленности о киберзащите. Постановлением № 3611 INCB также было поручено «продвигать

и повышать осведомленность общественности об угрозах в киберпространстве и средствах борьбы с ними». Один из подходов к достижению этого заключался в организации и финансировании конференций INCD или Министерством иностранных дел (например, «Кибер-неделя» или «Кибертех»). Их цель — обсудить киберпроблемы и повысить осведомленность о киберугрозах. Другой подход заключался в повышении осведомленности и уровня знаний через частный сектор. Наконец, образовательные программы помогают повысить осведомленность израильского общества.

Образовательные и обучающие программы по киберзащите. Согласно Постановлению правительства № 3611 образование являлось еще одной обязанностью INCB (2011 г.). Совместно с Армией обороны Израиля и Министерством образования оно разработало различные программы, ориентированные на молодых израильтян. Среди них есть две внешкольные киберпрограммы — *Magshimim* и *Nitzanei Magshimim*, которые помогают формировать, выявлять и привлекать молодые таланты. Действительно, 75% студентов, прошедших одну из этих программ, позже служат в кибервразведывательных подразделениях ЦАХАЛа (2018 г.). Третья программа *Gvahim* дополняет гражданское киберобразование и готовит учащихся к вступительному экзамену в среднюю школу по кибербезопасности, информатике и математике.

ЦАХАЛ также разработал два курса для обучения своих киберсолдат. Часть отличников получают диплом инженера, финансируемого Армией обороны Израиля, прежде чем пойти в армию, но должны проработать еще от трех до пяти лет. Другой трек «Тальпиот» — это 40-месячная программа элитной подготовки для выдающихся старшеклассников, проводимая Управлением оборонных исследований и разработок.

После службы солдаты зачастую успешно попадают в частный сектор высоких технологий и получают дополнительный опыт. Поскольку они являются частью резервных сил ЦАХАЛа до достижения возраста 40–50 лет, армия также получает прибыль от этой части своего учебного процесса.

Раздел II
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ

И.Л. Хромов, Н.А. Кузьмин, И.А. Завьялов

Перспективные направления использования искусственного интеллекта в оперативно-розыскной деятельности

В настоящее время современное развитие науки и техники неминуемо влечет за собой изменение средств и методов борьбы с преступностью. Развитие системы искусственного интеллекта (далее — ИИ) в разнообразных сферах деятельности нашей страны показывает ее возрастающую актуальность, эффективность и, как следствие, востребованность для использования ОВД при осуществлении ОРД.

Президент Российской Федерации В.В. Путин, выступая 4 декабря 2020 г. на международной онлайн-конференции *Artificial Intelligence Journey* (*AI Journey*), проводимой Сбербанком совместно с ведущими российскими и зарубежными компаниями, заявил: «Искусственный интеллект, безусловно, это основа очередного рывка вперед всего человечества в своем развитии». Глава государства подчеркнул, что «надо смело вести научный поиск там, где перспективы исследования пока еще неосязаемы», и обозначил задачи государства, заявив, что «в наступающем десятилетии нам предстоит провести цифровую трансформацию всей страны, всей России, повсеместно внедрить технологии искусственного интеллекта, анализа больших данных»[1].

В Национальной стратегии развития искусственного интеллекта на период до 2030 года под искусственным интеллектом понимается комплекс технологических решений, позволяющий имитировать когнитивные функции человека (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые как минимум с результатами интеллектуальной деятельности человека[2].

---

[1] Конференция по искусственному интеллекту // Официальный сайт Президента России. URL: http://www.kremlin.ru/events/president/news/64545 (дата обращения: 05.02.2021).

[2] См.: Национальная стратегия развития искусственного интеллекта на период до 2030 года: утв. Указом Президента РФ В.В. Путина от 10 октября 2019 г. № 490 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_335184/ (дата обращения: 22.12.2020).

Искусственный интеллект — это вычислительная платформа для выполнения конкретных, заранее заданных функций и решения задач, устройство превращения любой — визуальной, акустической, текстовой и т.п. — информации в цифру, обработка этой цифры методами статистики и дискретной вычислительной математики и получение ответа в интуитивно понятном для человека виде[1]. Именно искусственный интеллект является основой для сбора, хранения и обработки информации.

Не вызывает сомнений, что одной из сфер, где должны активно внедряться возможности технологий ИИ, является ОРД.

В настоящее время в мире выделяют два основных направления развития ИИ[2].

Первое направление — так называемый «универсальный» (сильный) ИИ, который в полном объеме способен заменить человека, в настоящее время только исследуется и перспективы его применения не совсем ясны. Второе направление — так называемый «слабый» ИИ, на основе которого создаются полностью автоматизированные системы, который развивается в последнее время очень интенсивно. В рамках этого направления ИИ не заменяет человека, а решает конкретные задачи, связанные с распознаванием, установлением взаимосвязей на основе матричных и статистических методов и т.п.

Применительно к ОРД возможности ИИ используются в основном для сбора, хранения и обработки информации; построения различных аналитических и прогнозных моделей, а также для обеспечения коммуникации и взаимодействия.

В быстро меняющемся мире ИИ становится действенным инструментарием ОРД в борьбе с преступностью. Это в первую очередь обусловлено тем, что ИИ невозможно подкупить или убедить его в чем-то, скрыть выявленное преступление. Принимаемые ИИ решения обусловлены конкретными алгоритмами, которые тяжело изменить или перенастроить.

Подобные системы уже показали свою эффективность в других странах. В настоящее время мировым лидером в исследованиях ИИ являются США. В аналитико-ситуационных центрах полиции США оборудована программно-аппаратная среда для накопления,

---

[1] См.: *Овчинский В.С., Ларина Е.С.* Искусственный интеллект. Большие данные. Преступность («Коллекция Изборского клуба»). М.: Книжный мир, 2018. С. 4.

[2] *Овчинский В.С., Маслов А.А., Бабушкин А.А.* О перспективах использования технологий искусственного интеллекта в оперативно-розыскной деятельности органов внутренних дел: науч. доклад (ВНИИ МВД России, 2020).

хранения и обработки информации о лицах, в которой содержатся различные сведения, такие как фотографии, голосовые данные и т.п.

В Нью-Йорке еще в 2007 г. был создан централизованный операционный центр общественной безопасности, в который было интегрировано более 100 разрозненных источников данных. Информация из различных источников, таких как камеры видеонаблюдения, патрульные машины, звонки в полицию и др., представленная в неструктурированном виде, поступает в центр и преобразуется в универсальный формат. Затем этот массив информации анализируется, структурируется и распределяется согласно запросам пользователей. Как уверяют разработчики, создание единого хранилища информации позволило снизить преступность в городе на 27%. Кроме того, был создан сервис поиска оперативно-значимых данных из источников информации, которые из-за своей разрозненности, различной формы и несочетаемости ранее не структурировались: заявления граждан, различные отчеты полиции, записи телефонных звонков, поступавших на номер 911, протоколов арестов и др. Все эти данные не были объединены, и выявление в них нужных сведений и взаимосвязей было затруднено. Результатом создания центра стало также повышение эффективности работы полиции[1].

Весьма актуальными являются аналитические и прогнозные возможности ИИ при осуществлении ОРД.

Так, во многих городах США (например, в Лас-Вегасе) внедрены системы анализа данных, выявляющие тенденции и предсказывающие вероятное время и место совершения преступлений. Используя отчеты о совершенных преступлениях, система определяет районы с наибольшей вероятностью совершения правонарушений, выделяет эти участки на карте и передает сотрудникам полиции на местах[2].

В нашей стране также существуют подобные системы, в частности функционирующая в г. Москве *АИС «Карта криминогенности»*. Она выполняет функции, аналогичные функциям американской программы, на основе мониторинга криминогенной обстановки в г. Москве. В частности, в режиме реального времени на карте отображаются места концентрации происшествий, выводится информация о каждом правонарушении и преступлении

---

1 *Жданов Ю., Овчинский В.* Полиция будущего. М., 2018.

2 *Жданов С.* Вы арестованы за намерение. Как новейшие цифровые разработки помогают предсказывать и предотвращать преступления // НОЖ. URL: https://knife.media/predict-crime/ (дата обращения: 07.01.2021).

по видам, составу данных (преступниках, потерпевших), местах концентрации и т.д. При этом система способна отображать информацию о происшествиях и преступлениях в виде тепловой карты по округам и районам города. Отдельно следует отметить функцию системы по осуществлению мониторинга присутствия иностранных граждан на территории г. Москвы.

Приведенные возможности АИС «Карта криминогенности», работа которой строится на основе ИИ, позволяют оперативным сотрудникам анализировать оперативную обстановку на конкретной территории в режиме реального времени, планировать ОРМ по предупреждению, выявлению и раскрытию конкретных преступлений, а также определять места оперативного прикрытия объектов и территорий и т.д. Вместе с тем отметим, что возможности данной системы ограничены агломерацией г. Москвы и, к сожалению, не в полной мере задействуются при осуществлении ОРД.

Еще одним перспективным направлением использования возможностей искусственного интеллекта в ОРД являются уже эффективно функционирующие в других странах технологии, позволяющие в режиме реального времени автоматически выполнять аналитическую деятельность по профилактике и раскрытию преступлений. В частности, в США функционирует система интеллектуального предупреждения преступлений Domain Awareness System, которая собирает и анализирует информацию с камер, линейных радаров, сенсоров и баз данных правоохранительных органов, при этом она позволяет в режиме реального времени наблюдать, например, за задержанием подозреваемых или иными их действиями, а также фиксировать неочевидные на первый взгляд моменты. Информация в систему поступает с 3 тыс. видеокамер, 2,6 тыс. датчиков и сенсоров полиции[1].

Наряду с положительным опытом использования систем ИИ в США, сегодня нельзя не отметить ведущие позиции Китая на данном направлении. Развитие технологий, связанных с ИИ, в этой стране определяется как важная внутриполитическая задача. На их использовании основана созданная в Китае система контроля над поведением граждан (система социального доверия), которая призвана обеспечить социально-политическую стабильность и гарантии сохранения политического строя Китая. Главным преимуществом КНР в мировой гонке за лидерство в сфере ИИ (в дополнение к огромным финансовым вложениям в отрасль) яв-

[1] Domain Awareness System // Tadviser. URL: https://www.tadviser.ru/index.php/Продукт:Domain_Awareness_System (дата обращения: 14.01.2021).

ляется огромный объем данных, генерируемых китайскими пользователями и используемых правоохранительными органами в своей повседневной деятельности.

Ярким примером использования аналитических и прогнозных моделей, применяемых в КНР, является разработанная компанией «Cloud Walk» (Гуанчжоу) система распознавания лиц, которая отслеживает действия людей. Исходя из того, когда и куда подозреваемый ходил и что делал, система может выдать вероятность совершения преступления.

В этом направлении в нашей стране также имеются достаточно серьезные наработки. В частности, в столице нашего государства, г. Москве, который является лидером среди российских городов по использованию систем искусственного интеллекта, успешно функционирует система *АПК «Безопасный город»*. Благодаря использованию систем видеонаблюдения информационно-поисковой системы «Безопасный город» в Москве эффективно решаются вопросы обеспечения безопасности при проведении массовых мероприятий, охране общественного порядка, а также вопросы выявления, предупреждения и раскрытия преступлений и правонарушений.

В результате деятельности оперативных подразделений Главного управления МВД России по г. Москве с использованием системы АПК «Безопасный город» в 2020 г. было раскрыто 5085 преступлений, из них 2713 краж, 40 убийств, 129 фактов умышленного причинения тяжкого вреда здоровью, 201 разбойное нападение, 516 грабежей[1].

Наряду с этим можно без преувеличения сказать, что при раскрытии большинства преступлений общеуголовной направленности в городе оперативные сотрудники используют в той или иной степени имеющиеся возможности системы АПК «Безопасный город». Это во многом обусловлено тем, что в городе создана уникальная материально-техническая база. Так, в рамках АПК «Безопасный город» функционирует *ГИС «Единый центр хранения данных»*, в которую по состоянию на 1 января 2021 г. было интегрировано 200 209 видеокамер, из которых 197 113 видеокамер установлены в г. Москве, 3096 видеокамер — в Московской области.

[1] Здесь и далее используются данные: Примеры положительного использования полицией города Москвы Подсистемы регистрации сценариев индексирования видеоинформации Государственной информационной системы «Единый центр хранения и обработки данных» Парсив ГИС «ЕЦХД». М.: ГУ МВД России по г. Москве, 2021. С. 3.

Имеющиеся технические возможности позволяют достаточно эффективно решать задачи по борьбе с преступностью, поскольку камеры контролируют наиболее значимые и важные объекты городской инфраструктуры. Так, более 100 000 камер установлены перед входами в подъезды (почти 90% от числа всех жилых домов города), около 24 тыс. камер контролируют придомовые территории. Большое количество камер расположено в местах с массовым скоплением граждан (6301), в образовательных организациях (12 330), на торговых объектах (6394); на объектах здравоохранения и социальной сферы (13 637); на стадионах (3832), в парковых зонах (2717). Помимо этого, в систему интегрированы камеры московского метрополитена и камеры интеллектуальной транспортной системы (4214).

С каждым годом возможности АПК «Безопасный город» постоянно совершенствуются, что позволяет ставить под контроль камер видеонаблюдения территорию торговых центров, спортивные и другие объекты.

Разносторонний охват различных объектов камерами системы АПК «Безопасный город» позволяет оперативным сотрудникам эффективно использовать ее не только для борьбы с преступлениями общеуголовной направленности. Увеличение в последние годы числа преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, заставляет задуматься о преломлении возможностей системы АПК «Безопасный город» для борьбы, например, с дистанционными хищениями средств с банковских карт и банкоматов. Такая деятельность неминуемо приведет к необходимости совершенствования возможностей системы АПК «Безопасный город». Очевидно, что для этого необходимо будет продолжать интеграцию всех установленных в городе на различных объектах локальных систем видеонаблюдения, а именно систем видеонаблюдения органов исполнительной власти города, государственных, муниципальных, банковских, коммерческих организаций, социальных учреждений, объектов транспортной инфраструктуры, в единую платформу, а также потребуется увеличение возможностей систем ИИ в АПК «Безопасный город». Причем искусственный интеллект, применяемый в АПК «Безопасный город», будет не только способствовать выявлению и раскрытию преступлений, но и во многом обеспечивать их профилактику. Этому будет способствовать использование уже имеющихся примеров анализа видеоархивов на предмет выявления и отождествления лиц по биоантропометрическим признакам. В настоящее время уже ведется обработка видеоархивов с возможностью поиска интересующего

лица с использованием функции биометрии, которой оснащены камеры на входе в подъезды. Можно загрузить фотографию с любого носителя информации, после чего будет получена информация об имеющихся совпадениях. Кроме того, есть возможность анализа движения по геометрии в кадре с использованием функции «пересечение линии» и движения в «выделенной зоне». Данные процессы сегодня не могли бы быть реализованы без использования систем искусственного интеллекта. Все это позволяет не только осуществлять розыск скрывающихся преступников, но и получать оперативно значимую информацию об интересующем объекте (маршрут его передвижения, контроль нахождения по конкретному адресу и т.д.).

В 2020 г. в г. Москве модуль видеоаналитики Парсив ГИС «ЕЦХД» использовался в 20 067 случаях при проведении ОРМ, установлении обстоятельств преступлений и примет предполагаемых преступников. В рамках его работы при осуществлении мероприятий по отождествлению лиц, находящихся в федеральном розыске, в 2020 г. было идентифицировано 280 изображений лиц, подтверждена личность и задержаны 263 субъекта. При проведении 47 массовых мероприятий с использованием системы видеонаблюдения выявлено 52 лица, представляющих интерес для сотрудников полиции, в том числе 11 лиц, находящихся в федеральном розыске, 12 лиц, находящихся под административным надзором, 11 лиц по базе данных ЦПЭ и 16 лиц, имеющих запрет на посещение массовых и спортивных мероприятий[1].

Получение таких результатов при использовании видеоаналитики распознавания лиц в г. Москве было бы невозможным, во-первых, без соответствующей материально-технической базы, а во-вторых, без четких сценариев действий сотрудников органов внутренних дел в той или иной ситуации. Что касается первой составляющей, то в городе за последние несколько лет была проделана колоссальная работа по наращиванию количества камер с функцией видеоаналитики (на сегодняшний день это более 100 000 камер подъездного видеонаблюдения, 500 камер, установленных в общественных местах, 1500 камер на объектах проведения мероприятий — контрольно-пропускные пункты стадионов, рамки

[1] Примеры положительного использования полицией города Москвы Подсистемы регистрации сценариев индексирования видеоинформации Государственной информационной системы «Единый центр хранения и обработки данных» Парсив ГИС «ЕЦХД». М.: ГУ МВД России по г. Москве, 2021. С. 5.

на массовых мероприятиях и пр.)[1]. Представляется, что имеющиеся возможности будут ритмично преумножаться, что позволит обеспечить эффективное функционирование системы видеоаналитики в последующем.

Весьма важным направлением использования ИИ в ОРД является противодействие коррупции. На фоне продолжающегося распространения коррупционных преступлений ИИ становится действенным инструментарием для противодействия деятельности нечистых на руку чиновников.

Сегодня программы, работающие с использованием ИИ, позволяют не только определять по подозрительной банковской активности потенциальную взятку, но и прогнозировать развитие коррупции задолго до ее появления. ИИ помогает также найти в различного рода документации, прежде всего финансового, бухгалтерского характера, сведения, свидетельствующие о причастности отдельных лиц к совершению коррупционных преступлений, либо иную информацию, указывающую на коррупционные факты, а также противоправные действия чиновников.

Подобные системы уже показали свою эффективность в других странах. И здесь особенно ценен опыт Китая на этом направлении. Развернутая в пилотном варианте *система ИИ* «*Zero Trust*» позволила выявить тысячи коррупционеров и получить конкретные доказательства их преступной деятельности.

Работа данной системы была построена на основе сопоставления множества баз данных федерального и регионального уровней с доходами и расходами государственных служащих. Это позволило с высокой долей эффективности выявлять наиболее характерные и распространенные коррупционные правонарушения, связанные с незаконной передачей прав собственности на имущество, со злоупотреблениями в сфере земельных отношений, махинациями при проведении различного рода тендеров и т.д. Безусловно, при обработке большого количества различных данных система ИИ «Zero Trust» не могла однозначно указывать на совершение коррупционного преступления или правонарушения, и решающий вывод был за оператором. В связи с этим можно сделать вывод, что ИИ, обрабатывая большие объемы данных, дает возможность оператору сосредоточиться на важных, имеющих значение деталях, которые

[1] Результаты совместной работы правительства Москвы и ГУ МВД России по городу Москве по использованию и развитию городской системы видеонаблюдения в интересах обеспечения правопорядка и общественной безопасности на территории города. М.: Департамент информационных технологий г. Москвы, 2020. С. 1.

свидетельствуют о наличии или отсутствии признаков коррупционных преступлений.

Несмотря на высокую эффективность подобных программ для борьбы с коррупцией, их использование вызывает и ряд вопросов. Так, очевидно, что для определения фактов коррупции, в основе которого лежит сопоставление сведений о доходах и расходах чиновников и информации, содержащейся в различных базах данных, ИИ потребуется анализировать информацию, находящуюся не только в государственных органах, но и в других организациях, в том числе банках. Соответственно, неминуемо возникают вопросы правового характера. Например, согласно ст. 26 Федерального закона от 2 декабря 1990 г. № 395-1 «О банках и банковской деятельности» кредитная организация, Банк России, организация, осуществляющая функции по обязательному страхованию вкладов, гарантируют тайну об операциях, о счетах и вкладах своих клиентов и корреспондентов[1]. Закономерно встает вопрос о доступе системы ИИ к данным таких организаций без каких-либо ограничений. Этот вопрос представляется чрезвычайно важным, поскольку сегодня сохраняются тенденции уменьшения доли наличных денежных средств при каких-либо действиях коррупционеров по легализации преступно нажитых денежных средств (операциях по купле-продаже товаров и услуг, недвижимости и т.д.). Системы отслеживания транзакций интересующих фигурантов, ввода и вывода денежных средств при помощи искусственного интеллекта могут охватить практически все траты конкретного лица. И если раньше такие мероприятия требовали использования значительных ресурсов для проверки сведений о доходах и расходах чиновников, в частности направления запросов в различные ведомства, то теперь искусственный интеллект может существенно сократить время проведения таких проверок. В результате для анализа оператору будут поступать совершенно конкретные факты, свидетельствующие, например, о том, что чиновник совершает траты денежных средств в значительных объемах, их переводы либо получает на свой счет необоснованные суммы денег и т.д.

Бесспорно, при создании подобной системы ИИ в России органы внутренних дел смогут получить дополнительный инструментарий для противодействия коррупционным преступлениям, что

[1] См.: О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. № 395-1 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5842/ (дата обращения: 28.12.2020).

позволит своевременно реагировать на имеющуюся информацию и принимать необходимые меры.

Таким образом, можно констатировать, что все ведущие государства, в том числе и Россия, видят в создании систем ИИ огромный потенциал для развития своей экономики и военной мощи, разрабатывают стратегии его развития, принимают соответствующие нормативные правовые акты, регулирующие отношения в сфере ИИ, и вкладывают в его развитие огромные ресурсы.

Эффективное применение технологий ИИ в сфере ОРД позволит обеспечить более качественное и эффективное противодействие преступлениям, в том числе совершаемым с использованием информационно-телекоммуникационных технологий.

Вместе с тем функционирование систем ИИ в правоохранительной деятельности в целом и в ОРД в частности носит не в полной мере системный характер и требует решения целого ряда вопросов.

Так, необходима интеграция всех имеющихся в настоящее время учетов, как открытых, хранением и систематизацией которых занимаются ГИАЦ МВД России и ЭКЦ МВД России, так и закрытых — оперативно-справочных, функции по ведению которых в настоящее время возложены на БСТМ МВД России, с целью проведения интеллектуального анализа разнородной информации применительно к процессу раскрытия преступлений. Кроме того, требуют серьезного развития системы автоматизированного поиска и анализа контента в сети Интернет с последующим его сравнением с имеющимся массивом информации о совершенных преступлениях и разыскиваемых лицах.

Развитие комплексных систем, способных в режиме реального времени проводить идентификацию граждан по биометрическим данным (отпечаткам пальцев и ладоней рук, изображениям лиц и радужной оболочке глаза, татуировкам, шрамам, голосовым файлам и др.) или прогнозировать их поведение, должно идти в масштабах всех субъектов страны.

Наряду с этим необходимо качественное преломление использования имеющихся систем ИИ в коммерческих и государственных структурах для целей ОРД (банки, Росфинмониторинг, социальные сети, мессенджеры, интернет-провайдеры, медицинские учреждения и т.п.).

При этом необходимо нормативное регулирование данного сектора, установление эффективной системы контроля, позволяющей соблюсти права и свободы человека, не допустить утечек данных и контролировать процессы принятия решения ИИ.

В.В. Агеев

Хакатон «Искусственный интеллект на службе полиции»

Процессы цифровой трансформации в Министерстве внутренних дел Российской Федерации, высокая потребность в быстром создании и развитии цифровых продуктов, управлении цифровыми услугами обусловливают необходимость постоянного совершенствования форм и методов работы ФКУ «ГИАЦ МВД России».

Мы посчитали очень важным и логичным привлечь к решению задач по внедрению систем ИИ и методов машинного обучения в процессы выявления, предупреждения и раскрытия преступлений именно представителей так называемого поколения NEXT, которое характеризуется прежде всего глубокой вовлеченностью в цифровые технологии. В связи с этим было принято решение о проведении ***первого в истории ведомства хакатона «Искусственный интеллект на службе полиции»***[1], итоги которого были подведены 20 мая 2021 г.

Основной целью проводимого нами хакатона являлось повышение эффективности оперативно-служебной деятельности подразделений МВД России за счет использования новейших технологий цифровой трансформации.

При этом мы были крайне заинтересованы в том, чтобы пригласить поучаствовать в реализации этих задач продвинутых, одаренных молодых людей — разработчиков программного обеспечения.

Заявки на участие в хакатоне поступили от 15 команд, сформированных из наиболее подготовленных курсантов Московского университета МВД России имени В.Я. Кикотя, Краснодарского и Санкт-Петербургского университетов МВД России, Воронежского института МВД России, а также трех команд Военно-космической академии имени А.Ф. Можайского Минобороны России. В качестве поддержки — опытные преподаватели образовательных

[1] Справочно: хакатон (англ. *hackathon* — от *hacker* «хакер» + *marathon* «марафон») — технический конкурс для разработчиков программного обеспечения, в ходе которого специалисты сообща решают какую-либо проблему на время.

организаций. За командами были закреплены кураторы из числа сотрудников ФКУ «ГИАЦ МВД России».

В течение месяца курсанты — в качестве разработчиков, проектировщиков, тестировщиков и дизайнеров программного обеспечения — создавали проекты автоматизированной информационной системы, использующей технологии ИИ для решения оперативно-служебных задач, связанных с предупреждением и раскрытием преступлений.

Участники не ограничивались в выборе тем проекта. Они сами обозначали проблему, разрабатывали техническое задание и реализовывали проект, демонстрируя полученные в ходе обучения навыки и знания в области искусственного интеллекта, машинного обучения, компьютерного зрения.

Специально для данного конкурса ФКУ «ГИАЦ МВД России» создан сайт «Хакатон». Для обмена мнениями на нем были размещены вся конкурсная документация, методические материалы: шаблоны презентации для защиты проекта, критерии оценки работ, указаны участники команд и разрабатываемые проекты. К примеру, для участия в конкурсе были заявлены такие проекты, как:

- «*Технология искусственного интеллекта распознавания подозрительных или угнанных, похищенных транспортных средств, в том числе водители которых скрылись с места происшествия*»;
- «*Интеллектуальная система поиска информации по человеку в социальных сетях*»;
- «*Автоматизированная информационная система "Криминалистическая профилактика преступлений", основанная на исследовании данных из сводок оперативных дежурных*»;
- «*Программный комплекс поддержки принятия решений на основе результатов анализа оперативной обстановки из различных источников в масштабе реального времени*»;
- «*Нейросетевой классификатор ролей пользователей в структурах пропаганды политического протеста в социальных сетях*»;
- «*Автоматизированная система интеллектуального отбора лиц, представляющих оперативный интерес*», «*Интеллектуальная система онлайн-проверки по документу, удостоверяющему личность*».

Новостная лента сайта информировала о стадиях проведения хакатона. Словом, портал сопровождал конкурсантов с момента регистрации до финальной презентации проектов и подведения итогов.

В жюри, которое оценивало работы, вошли представители ФКУ «ГИАЦ МВД России», ФКУ НПО «СТиС» МВД России, Ака-

демии управления МВД России, Московского государственного технического университета имени Н.Э. Баумана.

В итоге призовые места распределились следующим образом.

Третье место присуждено программистам в погонах из команд:

— «CopIB» Московского университета МВД России им. В.Я. Кикотя, осуществившей проект *интеллектуальной системы идентификации граждан*;

— «Star Track» Военно-космической академии имени А.Ф. Можайского, создавшей *интеллектуальную систему поддержки принятия решения по прогнозированию и раскрытию преступлений*;

— «IT-портрет» Воронежского института МВД России, реализовавшей проект *автоматизированной системы сбора и учета элементов внешности для изготовления субъективных портретов разыскиваемых лиц.*

Второе место заняли:

— команда «Ё-КУСП» Воронежского института МВД России с разработкой, позволяющей проводить *интеллектуальный анализ текстовых сообщений о преступлениях, правонарушениях и происшествиях*;

— команда «Souz Team» Военно-космической академии имени А.Ф. Можайского, спроектировавшая *сервис оперативного распознавания человеческой речи и семантического анализа текстов.*

Первое место в напряженной борьбе заняла команда «Василиск.AI» Московского университета МВД России им. В.Я. Кикотя с программой, способствующей *поиску похищенного антиквариата на открытых торговых онлайн-площадках.*

Приказом Министра внутренних дел генерала полиции Российской Федерации В.А. Колокольцева от 1 июня 2021 г. № 458л/с за победу в конкурсе-хакатоне «Искусственный интеллект на службе полиции» команда Московского университета МВД России им. В.Я. Кикотя «Василиск.AI» поощрена денежной суммой в размере 100 тыс. руб.

В отдельной номинации «За актуальность идеи» жюри была отмечена команда «LamerTeam» Краснодарского университета МВД России с *системой предиктивной аналитики, включающей поиск и получение данных для прогнозирования будущих криминальных событий.*

Планируется, что проект победителей «Применение технологий искусственного интеллекта при поиске антиквариата на открытых торговых онлайн-площадках» будет внедрен в деятельность подразделений органов внутренних дел.

Уже сегодня можно отметить положительный опыт проведенного нами конкурса, поэтому и в последующем мы также планируем организовывать подобные хакатоны, расширив круг участников и пригласив представителей других министерств и ведомств, высших учебных заведений.

Очевидно, что интерес к программным продуктам на основе ИИ в министерстве этим не ограничится. Поэтому, наряду с ежегодным проведением хакатона, мы решили организовать *постоянно действующую площадку* (*сообщество*) *для обмена мнениями и опытом в области цифровизации, повышения информационной безопасности — для IT-специалистов ведомства, учащихся научных и образовательных организаций.*

Разработчики программного обеспечения смогут обмениваться суждениями, решениями, повышая таким образом эффективность работы. При этом каждый наш территориальный орган будет иметь возможность размещать материалы, где сможет как раскрыть решение проблемы, с которой ему пришлось столкнуться, так и поделиться инициативными разработками.

Все это будет способствовать плодотворному сотрудничеству специалистов и дальнейшему развитию информационных технологий в Министерстве внутренних дел Российской Федерации.

А.А. Бабушкин, А.А. Маслов, В.С. Овчинский

О некоторых научных проблемах использования искусственного интеллекта в оперативно-розыскной деятельности

К концу 2020 г. более 35 стран, включая Россию, приняли национальные стратегии развития ИИ, а общий объем затрат на ИИ в мире в 2020 г. оценивается в 50 млрд долл. Такие активные с точки зрения геополитики игроки, как США, Китай, Великобритания, Япония, Индия, Франция, Германия, Канада, а также Евросоюз в целом, обозначают высокий приоритет ИИ в стратегиях национальной безопасности и инвестируют в это миллиарды долларов в рамках долгосрочных программ.

Не вызывает сомнений, что одной из сфер, где должны активно внедряться новые технологические платформы, основанные на методиках обработки «больших данных» и применении технологий ИИ, является правоохранительная деятельность, включая ее оперативно-розыскной сегмент.

Полицейские эксперты ОБСЕ об использовании ИИ преступниками и формировании новых подходов к организации полицейской деятельности на базе ИИ

23–24 сентября 2019 г. на *Ежегодной встрече полицейских экспертов ОБСЕ, в которой принимают участие представители полиции со всего мира и которая проходила в Вене*, впервые обсуждалась тема ***«Искусственный интеллект и правоохранительные органы: союзники или противники?»***. В выступлениях на форуме подчеркивалось, что достижения в области ИИ создают новые беспрецедентные возможности для правоохранительной и правоприменительной деятельности, прежде всего по направлению идентификации фигурантов или транспортных средств, связанных с уголовными делами и другими нарушениями. ИИ способствует повышению качества аналитики и прогнозирования криминальной деятельности, созданию эффективных комплексов противодействия поведенческой агрессии в виде манипулирования контент-

ными потоками, загрязнения информационного пространства фейками и т.п.

Обсуждение позволило четко сформулировать два в значительной степени не пересекающихся направления развития ИИ и робототехники.

Первое носит поисковый, исследовательский характер и на сегодняшний момент на нем отсутствуют сколько-нибудь значимые практические результаты. Речь идет о так называемом сильном ***(универсальном) ИИ***, в полном объеме способном заменить человека.

Другое направление развивается ошеломительными темпами. Это так называемый ***слабый ИИ*** и базирующиеся на нем полностью автоматизированные робототехнические системы. В рамках данного направления ИИ не стремится заменить человека по всей гамме его способностей и возможностей. Он решает конкретные задачи, связанные либо с распознаванием, либо с установлением взаимосвязей на основе матричных и статистических методов.

Слабый ИИ может быть уподоблен механическим вычислительным машинам, типа арифмометра, в том же смысле, в котором реактивный самолет может быть уподоблен воздушным шарам. ИИ и робототехника такого рода не стремятся полностью заменить человека. Их задача — научиться выполнять конкретные операции на несколько порядков лучше, чем человек.

На форуме также отмечалось, что развитие ИИ в полиции необходимо в связи с тем, что преступники все чаще берут на вооружение ИИ и робототехнику. В основном на сегодняшний день это происходит по трем направлениям:

— *во-первых*, ИИ используется высокотехнологичным криминалом при совершении сложных киберпреступлений, связанных либо с атакой на крупные торговые порталы, либо с попытками взять на себя управление объектами «Интернета вещей» — от дома до системы управления водохранилищами;

— *во-вторых*, на сегодняшний день повседневным стало использование управляемых с участием ИИ дронов и других робототехнических систем для перевозки преступных товаров, прежде всего наркотиков, человеческих донорских органов и т.п., а также для доставки запрещенных товаров на территорию тюрем и исправительных учреждений;

— *в-третьих*, и это представляет наибольшую угрозу для глобальной экономики, продвинутые преступники используют ИИ и боты для атак на финансовую инфраструктуру банков, инвестиционных компаний, финансовых институтов. В настоящее время уже

более 80% объема транзакций на рынках капитала осуществляется в рамках полностью автоматической торговли на базе электронных платформ. Преступники стремятся нарушить целостность этих платформ и либо украсть деньги, либо осуществлять манипуляцию рынками путем внесения изменений в программы.

Основной акцент в выступлениях был сделан на том, чем ИИ и робототехника могут быть полезны для правоохранителей. Здесь выделено *четыре главных направления*: сбор информации, хранение и обработка информации; аналитические и прогнозные модели; осуществление цифровых расследований; обеспечение коммуникаций и взаимодействия.

Все выступающие подчеркивали, что ИИ и робототехника — это в значительной степени обоюдоострый меч. Его могут использовать как полицейские, так и преступники, и тем более террористические группы. Вполне вероятно также, что *ИИ породит новые виды преступности, о которых мы пока не догадываемся*. Как показывают экспертные опросы, подавляющее большинство исследователей и практиков в области ИИ уверены, что любое решение, работающее на правоохранителей, может быть использовано в своих целях и криминалом.

С точки зрения использования ИИ в преступных целях выделяются три главных направления:

Первое — цифровые нападения. Они включают в себя как элементарный автоматизированный фишинг, так и разработку и применение многофункциональных платформенных вредоносных программ. Такие программы нацелены не только на проникновение в защищенные сети и изъятие информации из корпоративных сетей, но и на разрушение или перехват управления физическими структурами, управляемыми корпоративным или федеральным ИИ.

Второе — политические нападения. В современном мире это отнюдь не покушения или убийства политических деятелей. Это манипулирование коллективным поведением на основе создания эхо-интернет-камер, потоков фейковых новостей, запуска фальсифицированных видеороликов и фотографий и в целом дискредитация любой информации в сети, особенно той, которая могла быть использована в качестве доказательств, предъявляемых в суде.

Третье — физические нападения. Если раньше преступники нападали на человека, используя кулаки, ножи или пистолеты и винтовки, то сегодня уже зарегистрированы нападения с использованием «Интернета вещей». В Соединенных Штатах зафиксировано несколько случаев взятия под контроль при помощи вредоносного софта имплантатов — физических устройств, вживленных в чело-

веческое тело. Кроме того, для физических нападений, особенно террористами, используются дроны и беспилотные автомобили.

Риски криминальной эксплуатации ИИ

По мере расширения возможностей и развертывания технологий ИИ растут и риски его криминальной эксплуатации.

Для их оценки в США в феврале 2019 г. был проведен семинар на тему «Искусственный интеллект и преступность в будущем» (организован Центром борьбы с преступностью в будущем Дауэса при Калифорнийском университете в Лос-Анджелесе).

Участники семинара были разделены на группы по 4–6 человек, каждая из которых представляла собой баланс представителей различных профессий из академических кругов, правительства и промышленности. Работая в этих группах, эксперты оценивали возможные будущие преступления с использованием ИИ, разработанные командой организаторов, а также любые дополнительные преступления, совершенные в группах.

Преступления оценивались по четырем параметрам, которые были определены организационной группой на этапе анализа как полезные для понимания различных аспектов серьезности угрозы, а именно:

— *вред*: жертва и (или) социальный ущерб, при этом террор рассматривается как форма вреда. Например, финансовые потери для отдельного лица или подрыв доверия к государственным учреждениям будут считаться вредными последствиями;

— *преступная прибыль*: достижение преступной цели, например получение финансовой выгоды, террор, нанесение вреда или репутационный ущерб. Это может быть симметрично причинению вреда, хотя и не обязательно: преступление может иметь целью получение денежной прибыли, но в качестве побочного эффекта разрушает репутацию человека;

— *достижимость*: насколько осуществимо преступление с учетом готовности необходимой технологии, ее доступности и практических сложностей сбора данных или требуемой инженерии. Например, зависит ли возможность его совершения от очень дорогого оборудования или доступа к секретной информации;

— *побеждаемость*: меры по предотвращению, обнаружению или снижению прибыльности. Следует рассмотреть вопрос о том, не очевидны ли меры поражения; простой или сложный; и (или) нуждаются в изменении поведения. Например, может ли такая компания, как *Google*, ненавязчиво обойти преступление или для этого

требуется, чтобы каждый пользователь компьютера в мире был оснащен биометрическим сканером.

В 2020 г. обобщены результаты экспертных оценок.

Криминальный потенциал ИИ. ИИ может быть причастен к преступлениям, совершенным разными способами. Совершенно очевидно, что ИИ можно применять в качестве инструмента для совершения преступлений, используя его возможности для облегчения действий против реальных целей: прогнозирования поведения людей или учреждений с целью обнаружения и использования уязвимостей; создания поддельного контента в целях шантажа или нанесения вреда репутации; выполнения действий, которые преступники-люди не могут или не хотят осуществлять сами в силу опасности, физического размера, скорости реакции и т.д. Хотя методы и являются новыми, сами преступления могут быть традиционного типа — воровство, вымогательство, запугивание, террор.

В качестве альтернативы системы ИИ могут сами выступать целью преступной деятельности: обход защитных систем, которые создают препятствия для совершения преступления; уклонение от раскрытия или преследования за уже совершенные преступления; выведение из строя доверенных или критических систем либо провоцирование их неустойчивого поведения, чтобы нанести ущерб или подорвать доверие общества.

ИИ может также просто предоставить контекст для преступления. Мошеннические действия могут зависеть от того, что жертва считает, что некоторые функции ИИ возможны, даже если это не так, или они возможны, но фактически не используются в мошенничестве.

Конечно, эти категории не исключают друг друга. Как и в старой поговорке о поимке вора, для атаки на систему ИИ может потребоваться срабатывание системы ИИ. Мошенническое моделирование несуществующих возможностей ИИ может быть выполнено с использованием других существующих методов ИИ.

Преступления очень разнообразны. Они могут быть нацелены на частных лиц или учреждения, предприятия или клиентов, собственность, правительство, социальную структуру, общественный дискурс. Они могут быть мотивированы финансовой выгодой, приобретением власти или изменением статуса по отношению к другим. Они могут создавать или портить репутацию или отношения, менять политику или сеять разлад; такие эффекты могут быть самоцелью или ступеньками к какой-то дальнейшей цели. Они могут быть совершены для смягчения наказания или как по-

пытка избежать наказания за другие преступления. Они могут быть продиктованы желанием отомстить или достичь религиозных, политических целей или же сексуального удовлетворения. Они могут выражать всего лишь не что иное, как нигилистическое побуждение к разрушению, вандализму или насилию.

Степень, в которой это разнообразие преступных действий может быть увеличено за счет использования ИИ, в значительной мере зависит от того, насколько они встроены в вычислительную среду: робототехника быстро развивается, но ИИ лучше подходит для участия в банковском мошенничестве, чем в драке в пабе. Такое предпочтение цифрового мира, а не физического является слабой защитой, хотя современное общество сильно зависит от сложных вычислительных сетей, причем не только для финансов и коммерции, но и для всех форм коммуникации, политики, новостей, работы и социальных отношений. В настоящее время люди проводят большую часть своей жизни в интернете, получают большую часть информации оттуда, и их активность в сети может создавать и разрушать их репутацию. Эта тенденция, вероятно, сохранится в обозримом будущем. Такая онлайн-среда, где данные являются собственностью, а информация — силой, идеально подходит для использования ИИ в преступных целях, и это может иметь серьезные последствия в реальном мире. Более того, в отличие от многих традиционных преступлений, преступления в цифровой сфере часто легко воспроизводимы: однажды разработанные методы можно распространять, повторять и даже продавать, что создает потенциал для маркетинга преступных методов или предоставления преступления как услуги. Это может привести к снижению технологических барьеров, поскольку преступники смогут передать на аутсорсинг более сложные аспекты своей преступной деятельности с использованием ИИ.

Дипфейки. Люди склонны верить своим собственным глазам и ушам, поэтому аудио- и видеосвидетельствам традиционно уделяется большое внимание (и часто это имеет юридическую силу), несмотря на долгую историю фотографических уловок. Но недавние разработки в области глубокого обучения значительно расширили возможности для создания поддельного контента. Уже можно сфабриковать убедительное олицетворение целей по фиксированному сценарию, и ожидается, что за этим последуют интерактивные олицетворения. Эксперты предусмотрели широкий спектр криминальных приложений для такой технологии «дипфейка», чтобы использовать безоговорочное доверие людей к этим СМИ (выдача себя за детей престарелых родителей с помощью видеозвонков для

получения доступа к средствам; использование телефона для запроса доступа к защищенным системам, фальшивые видео предосудительно действующих публичных деятелей с целью манипулирования поддержкой).

Воспроизведение аудио и видео с выдачей себя за другое лицо было признано наиболее опасным видом преступлений из всех рассмотренных и получило высокие оценки по всем четырем параметрам. Следовательно, изменения в поведении граждан могут быть единственной эффективной защитой. Эти поведенческие сдвиги, такие как общее недоверие к визуальным свидетельствам, можно рассматривать как косвенный общественный ущерб, причиненный преступлением, помимо прямого вреда, такого как мошенничество или ущерб репутации. Если окажется, что даже небольшая часть визуальных доказательств является убедительной фальшивкой, становится намного проще дискредитировать подлинные доказательства, подрывая уголовное расследование и доверие к политическим и социальным институтам, которые полагаются на достоверную информацию. Подобные тенденции уже проявляются в дискурсе вокруг «фейковых новостей». Прибыль была оценена как наименьшее из измерений этого преступления.

Беспилотные автомобили как оружие. Автомобили уже давно используются и как средство доставки взрывчатых веществ, и как собственно кинетическое оружие террора, причем последнее сейчас становится все более распространенным. Транспортные средства гораздо более доступны в большинстве стран, чем огнестрельное оружие и взрывчатые вещества, и автомобильные атаки могут быть предприняты с относительно небольшими организационными издержками фрагментарными, квазиавтономными террористами или террористами-одиночками, такими как террористы, заявляющие о своей принадлежности к ИГИЛ. Эта тактика получила особую известность после серии атак в западных городах, включая Ниццу (2016 г.), Берлин (2016 г.), Лондон (2017 г.), Барселону (2017 г.) и Нью-Йорк (2017 г.).

Хотя полностью автономные беспилотные автомобили с управлением от ИИ пока недоступны, многочисленные производители автомобилей и технологические компании стремятся их создавать, а некоторые из них разрешены для испытаний на дорогах общего пользования. Уже задействованы более ограниченные возможности автономного вождения, такие как вспомогательная парковка и управление полосой движения. Автономные транспортные средства потенциально позволили бы расширить возможности терроризма на транспортных средствах за счет уменьшения по-

требности в найме водителей. Так, отдельные злоумышленники смогли бы совершать несколько атак, даже координируя большое количество транспортных средств одновременно. Беспилотные автомобили обязательно будут включать в себя обширные системы безопасности, которые необходимо будет обходить, поэтому атаки без водителя будут иметь более высокий барьер для проникновения, чем в настоящее время, что потребует технологических навыков и организации. Тем не менее делегаты оценили эти атаки как весьма достижимые, вредные и умеренно прибыльные (учитывая террор как цель). Однако они получили низкие баллы по поражаемости (что означает относительную легкость), поскольку ожидается, что они будут восприимчивы к одним и тем же контрмерам.

Индивидуальный фишинг. Фишинг — это атака «социальной инженерии», целью которой является сбор защищенной информации или установка вредоносного ПО с помощью цифрового сообщения, которое якобы отправлено доверенным лицом, например банком пользователя. Злоумышленник использует существующее доверие, чтобы убедить пользователя выполнить действия, которых он в противном случае мог бы опасаться, например раскрытие паролей или переход по сомнительным ссылкам. Хотя некоторые атаки могут быть нацелены на конкретных людей, что называется «целевым фишингом», это не особо распространено. В настоящее время большинство фишинговых атак носят относительно неизбирательный характер, для них используются общие сообщения, стилизованные под основные бренды или тематические события, которые, как можно ожидать, могут заинтересовать некоторую часть пользователей чисто случайно. Злоумышленник полагается на простоту отправки огромного количества цифровых сообщений, чтобы превратить низкую частоту ответа в прибыль. Искусственный интеллект может повысить вероятность успеха фишинговых атак за счет создания сообщений, которые кажутся более подлинными (например, путем включения информации, полученной из социальных сетей, или путем подделки стиля доверенной стороны). Вместо того, чтобы посылать всем объектам единообразные сообщения, которые в большинстве случаев могут не попасть в цель, сообщения можно было бы адаптировать для использования конкретных уязвимостей, выявленных в отношении каждого человека, эффективно автоматизировав способ целевого фишинга. Кроме того, ИИ может использоваться в качестве метода активного обучения, чтобы обнаружить, «что работает», варьируя детали сообщений для сбора данных о том, как максимизировать ответы. Поскольку фишинговые атаки чаще всего совершаются с целью по-

лучения прибыли, преступление было оценено как имеющее лишь незначительно превышенный средний потенциал вреда, но при этом было высоко оценено с точки зрения прибыли, достижимости и поражаемости (что означает, что его будет трудно остановить).

Нарушение систем, управляемых ИИ. По мере того как расширяется использование ИИ в правительстве, бизнесе и рядовыми гражданами, а функции, выполняемые системами ИИ, становятся все более важными, возможности для атак будут расти. Системы, основанные на обучении, часто развертываются для повышения эффективности и удобства, а не для обеспечения надежности, и их нельзя априори признать критически важной инфраструктурой. Возможна масса криминальных и террористических сценариев, возникающих в результате целенаправленного нарушения работы таких систем, вызывающих массовые перебои в электроснабжении, тупиковое движение и нарушение логистики продовольствия. Системы, отвечающие за любые аспекты общественной безопасности, вероятно, станут ключевыми целями, как и те, которые контролируют финансовые операции. Соответственно, были высокие рейтинги прибыли и вреда, равно как и поражаемость. В целом, чем сложнее система управления, тем труднее полностью защищаться. Явление враждебных возмущений обостряет эту проблему, и достаточно продвинутые ИИ могут быть уязвимы для тщательно продуманных атак. Однако достижимость была оценена ниже на том основании, что такие атаки обычно требуют детального знания задействованных систем или даже доступа к ним, что может быть трудновыполнимо.

Масштабный шантаж. Традиционный шантаж представляет собой вымогательство под угрозой раскрытия доказательств совершения преступления или правонарушения или личной информации сомнительного содержания. Ограничивающим фактором традиционного шантажа является получение таких доказательств: преступление имеет смысл только в том случае, если жертва заплатит за сокрытие доказательств больше, чем стоит их приобретение. ИИ можно использовать для этого в гораздо большем масштабе, собирая информацию (которая сама по себе не должна выступать убедительным доказательством) из социальных сетей или больших наборов личных данных, таких как журналы электронной почты, история браузера, содержимое жесткого диска или телефона, а затем выявлять конкретные уязвимости для большого количества потенциальных целей и адаптации сообщений об угрозах для каждой. ИИ также может использоваться в целях создания фальшивых доказательств. Крупномасштабный шантаж получил

высокую оценку с точки зрения прибыли: как и в случае с фишингом, эффект масштаба означает, что атака может потребовать лишь небольшого количества попаданий, чтобы быть прибыльной. Победа считалась трудной, в основном по той же причине, по которой она проблематична в традиционных случаях: нежелание жертвы выйти вперед и столкнуться с уязвимостью. Однако ущерб был оценен только как средний, поскольку преступление по своей природе в первую очередь направлено против отдельных лиц. Достижимость также относительно низкая из-за высоких требований к данным и сочетания нескольких различных методов ИИ, которые необходимо координировать. Следует отметить, что среди современных методов фишинга распространен очень грубый аналог шантажа, не связанный с искусственным интеллектом. Термин «сексторция» означает ложное заявление о компрометирующей видеозаписи со взломанного компьютера или телефона пользователя. Как и в случае со всеми подобными мошенничествами, невозможно узнать процент попаданий, но мы подозреваем, что он довольно низкий.

Фейковые новости, созданные ИИ. Фальшивые новости — это пропаганда, направленная на то, чтобы вызвать доверие, поскольку они исходят из надежного источника или кажутся таковыми. Помимо предоставления ложной информации, фейковые новости в достаточном количестве могут отвлечь внимание от истинной информации. Делегаты рассмотрели возможность создания фальшивого новостного контента с помощью технологии искусственного интеллекта для достижения большей эффективности, присутствия или специфичности. ИИ можно использовать для создания множества версий определенного контента, очевидно, из нескольких источников, чтобы повысить его видимость и доверие к нему; и возможно выбирать контент или его представление на индивидуальной основе, чтобы усилить воздействие. Преступление получило оценку выше среднего по вреду, достижимости и поражаемости и ниже среднего по прибыли. Вред считался высоким из-за значительного потенциала влияния на конкретные политические события, например голосование (независимо от того, было ли это уже сделано), и из-за диффузных социальных эффектов, если передача реальных новостей подрывается или вытесняется фальшивыми СМИ. Высокая достижимость подчеркивалась в последних сообщениях семинара. Поражение считалось трудным как чисто техническая проблема, и потому что граница между фейком и реальными новостями нечеткая. На сегодняшний день наиболее успешные попытки борьбы с фейковыми новостями предпринимаются через об-

разование. Более низкий показатель прибыли отражает сложность получения финансовой выгоды от фальшивых новостей (хотя есть возможности для использования фальшивых новостей для манипулирования рынком) и обусловлен неопределенностью влияния его более расплывчатых последствий.

Военные роботы. Как и во многих областях технологического развития, военные гораздо более заинтересованы в исследованиях робототехники с потенциально очень разными целями, чем гражданские пользователи, несмотря на многие методологические совпадения. Можно ожидать, что любая доступность военной техники (например, огнестрельного оружия или взрывчатых веществ) для преступных или террористических организаций будет представлять серьезную угрозу, и это, безусловно, будет иметь место в случае автономных роботов, предназначенных для боевых действий или оборонительного развертывания. Эксперты оценили такой доступ как потенциально очень вредный и выгодный. Однако было также признано, что рейтинги были спекулятивными. Военные возможности обычно хранятся в секрете, и у нас очень ограниченные знания о текущем состоянии дел и темпах их продвижения.

Продажа мошеннических услуг под видом ИИ. Такое мошенничество чрезвычайно достижимо и практически не имеет технических барьеров (поскольку технология по определению не работает). Потенциальная прибыль высока: есть много печально известных примеров того, как мошенники продавали дорогостоящие технологические подделки крупным организациям, включая национальные правительства и вооруженные силы. Возможно, это не использование ИИ для совершения преступлений, но преступление зависит от того, верит ли его объект в заявленные возможности ИИ, что, в свою очередь, зависит от того, будет ли ИИ восприниматься общественностью как успешный инструмент. Это можно легко победить с помощью повышения уровня образованности и осмотрительности потенциальных жертв, однако в настоящее время, пока меры в этом отношении не приняты, злоумышленники имеют шанс на успех.

«Отравление» данных. Манипуляции с данными машинного обучения осуществляются для преднамеренного введения определенных предубеждений либо как самоцель (с целью нанести ущерб коммерческим конкурентам, исказить политический дискурс или сформировать недоверие в обществе), либо с намерением последующей эксплуатации. Например, возможно сделать автоматический рентгеновский детектор угроз нечувствительным к оружию, которое вы хотите переправить на борт самолета, или побудить

консультанта по инвестициям дать неожиданные рекомендации, которые изменят рыночную стоимость таким образом, чтобы у вас были предварительные знания, которые вы можете использовать. Чем шире используется источник данных и чем большее доверие он вызывает, тем более опасным он может быть. Хотя это преступление потенциально вредно и прибыльно, оно было оценено как низкое по степени достижимости, поскольку надежные источники данных, как правило, трудно изменить и (как следствие их широкого использования) они подвергаются частым проверкам.

Кибератаки на основе обучения. Существующие кибератаки имеют тенденцию быть изощренными и ориентированными на конкретную цель или грубыми, но сильно автоматизированными, основанными на огромном количестве цифр (например, распределенные атаки отказа в обслуживании, сканирование портов). ИИ повышает вероятность атак, которые являются как конкретными, так и массовыми, используя, например, подходы обучения с подкреплением для параллельного исследования слабых мест многих систем перед одновременным запуском нескольких атак. Такие атаки считались вредными и прибыльными, хотя делегаты были менее уверены в их достижимости.

Автономные боевые дроны. Неавтономные радиоуправляемые дроны уже используются для совершения таких преступлений, как контрабанда наркотиков в тюрьмы, а также становились причинами серьезных нарушений транспорта. Автономные дроны под управлением бортового ИИ потенциально позволяют повысить координацию и сложность атак, освобождая злоумышленника от необходимости находиться в пределах досягаемости передатчика дрона, что затрудняет нейтрализацию и задержание. В настоящее время дроны обычно не используются для совершения насильственных преступлений, но их масса и кинетическая энергия потенциально опасны при правильном нацеливании (например, в авиационные двигатели), и они также могут быть оснащены оружием. Дроны могут быть особенно опасными, если действуют массово самоорганизующимися роями. Они получили высокую оценку потенциального вреда, но низкую поражаемость, поскольку во многих контекстах защита может быть обеспечена с помощью физических барьеров.

Онлайн-выселение. Примат онлайн-активности в современной жизни, в сфере финансов, занятости, социальной активности и гражданства, представляет собой новую цель для атак против человека: отказ в доступе к тому, что стало важнейшими услугами, действует потенциально изнурительно. Это может быть использо-

вано как угроза вымогательства, чтобы нанести ущерб, или лишить права групп пользователей, или вызвать хаос. Некоторые злоумышленники посредством фишинговых и кибератак пытаются сделать нечто подобное с помощью таких средств, как «программы-вымогатели», и квазиорганизованные группы людей иногда участвуют в таких действиях, как массовое неверное сообщение о злоупотреблениях в социальных сетях, но ИИ может допускать и более тонкие — осторожные атаки (адаптация поддельной деятельности к нарушению условий обслуживания, определение конкретных уязвимостей для каждого человека), и более масштабируемые.

Обман распознавания лиц. Системы ИИ, которые выполняют распознавание лиц, все чаще используются для подтверждения личности на таких устройствах, как смартфоны, а также проходят испытания полицией и службами безопасности для таких задач, как отслеживание подозреваемых в общественных местах и ускорение проверки пассажиров на международных границах. Эти системы могут стать привлекательной мишенью для преступников. Было продемонстрировано несколько успешных атак, включая атаки «морфинга», которые позволяют одному удостоверению личности, например паспорту, передаваться (и использоваться) несколькими людьми. Прибыль и вред считались ниже среднего, поскольку атаки, скорее всего, позволят совершить относительно мелкие преступления.

Взрыв рынка. Обсуждалось манипулирование финансовыми или фондовыми рынками с помощью целевых, возможно, часто повторяющихся моделей сделок для нанесения ущерба конкурентам, валютам или экономической системе в целом (а не напрямую для получения прибыли от торговли, хотя это также может быть побочным эффектом). Обучение с подкреплением было предложено в качестве метода обнаружения эффективных торговых стратегий, возможно, в сочетании с медиа-анализом на основе создания поддельного контента. Достижимость была оценена как низкая из-за чрезвычайной сложности точного моделирования поведения рынка и очень высокой стоимости входа для участия в крупномасштабной торговле, но потенциальный ущерб и прибыль были соответственно высокими.

Использование предвзятости. Обнаружение и использование усвоенных (существующих) предубеждений в широко применяемых или влиятельных алгоритмах. Например, игровые рекомендации *YouTube* для направления зрителей к пропаганде или рейтинги *Google* для повышения узнаваемости продуктов или очернения конкурентов. На практике такое поведение уже широко рас-

пространено, часто не является незаконным (хотя оно может противоречить условиям обслуживания провайдера) и даже (в форме поисковой оптимизации или SEO) рассматривается как законная (хотя и сомнительная) бизнес-модель в интернете. Скорее всего, с помощью ИИ ее будет легче использовать и противодействовать ей.

Боты-взломщики. Небольшие автономные роботы, которые могут быть доставлены в помещения через небольшие точки доступа, такие как почтовые ящики или откидные дверцы для кошек, для извлечения ключей или открытия дверей и позволяют проникнуть внутрь людям-грабителям. Технические требования сильно ограничены, что должно сделать такие преступления более достижимыми, чем преступления, совершаемые с использованием более амбициозных классов автономных роботов. Но вред и прибыль невелики, потому что боты-взломщики позволяют совершать только очень локализованные, мелкие преступления, и их относительно легко можно победить с использованием простых физических средств, таких как почтовые ящики.

Уклонение от обнаружения ИИ. Ожидается, что полицейская служба и организации, обеспечивающие безопасность, будут все больше полагаться на сортировку и автоматизацию на основе ИИ для работы с постоянно растущими объемами данных, собираемых в ходе расследований. Атаки, которые подрывают эти процессы, чтобы стереть доказательства или иным образом помешать обнаружению, вероятно, станут все более привлекательными для преступников.

Состязательность возмущения (например, используемые для сокрытия порнографических материалов от автоматического обнаружения) предлагает один возможный путь к этому, хотя требования к знаниям системы могут быть непомерно высокими. Вред и прибыль были оценены как низкие, отчасти потому, что природа и контекст «преступления» были недостаточно определены, а сотрудники не были уверены в том, что это достижимо. Однако, если это было достигнуто, поражаемость оценивалась как трудная, поскольку преступление по определению сводится к тому, чтобы «избежать наказания за это».

Поддельные обзоры, созданные ИИ. Они используются для автоматического создания контента для таких сайтов, как *Amazon* или *TripAdvisor*, с целью формирования ложного (положительного или отрицательного) представления у клиентов о продукте или об услуге. Такие подделки уже совершаются человеческими агентами. ИИ может повысить эффективность, но прибыль и вред

от отдельных кампаний такого рода, скорее всего, останутся небольшими и локализованными.

Преследование с помощью ИИ. Это использование обучающих систем для отслеживания местоположения и активности человека через социальные сети или данные личных устройств. Считается также, что эта категория охватывает другие преступления, связанные с принудительными отношениями, домашним насилием, газлайтингом и т.д., и относится к текущим новостям, касающимся соучастия западных технологических компаний в предоставлении приложений для обеспечения соблюдения социальных норм в репрессивных обществах. Ущерб был оценен как низкий не потому, что эти преступления не являются чрезвычайно разрушительными, а потому, что они по своей сути сосредоточены на отдельных лицах и не имеют значимых возможностей для масштабных действий.

Подделка. Это создание поддельного контента, например произведений искусства или музыки, который может продаваться с указанием ложных сведений об авторстве. Данное деяние было оценено как наименьшая угроза из всех рассмотренных как с точки зрения вреда, так и вероятности успеха. Возможности искусственного интеллекта здесь остаются строго ограниченными: хотя был достигнут определенный успех в создании цифровых изображений, которые в целом имитируют визуальный стиль великих художников, это невозможно сравнить с созданием реальных физических объектов, которые прошли бы проверку в галерее или аукционном доме. Мир искусства веками сталкивался с подделками и имеет обширные (если не всегда достаточные) возможности защиты. ИИ даже не пытается устранить большинство из этих препятствий.

Структура рейтингов предполагает, что экспертов особенно беспокоили ***масштабируемые угрозы***, когда преступления, связанные с крупным ущербом отдельным лицам, обычно оценивались ниже, чем ущерб (возможно, меньший или нечетко определенный) большому количеству жертв, социальным группам или обществу в целом.

Использование ИИ и робототехники в правоохранительной и правоприменительной практике

Практическое использование началось с середины 10-х гг. XXI в. По этой причине между странами мира уже сложились и с каждым годом все четче проявляются различия в использовании правоприменительными и правоохранительными органами, в первую очередь полицейскими «на земле», достижений ИИ и робототехники. Ряд стран, прежде всего Соединенные Штаты, Великобритания, Китай,

Япония, Южная Корея, Израиль, не только создали в структуре правоохранительных органов ***центры адаптации ИИ и робототехники к повседневной работе правоохранителей***, но и широко осуществляют контакты с университетами и бизнесом как для создания полицейского софта с элементами ИИ, так и для обучения сотрудников правоохранительных органов ИИ и робототехнике.

Если подытожить практику работы подобных центров, то она демонстрирует, что в подавляющем большинстве случаев правоохранительные органы не используют какой-то уникальный, специально разработанный полицейский софт на базе ИИ, а адаптируют уже имеющиеся военные, разведывательные и бизнес-разработки под нужды полиции.

Среди технологий, которые уже вошли в повседневную жизнь сотрудников полиции, можно выделить в первую очередь:

- алгоритмы ИИ, нацеленные на распознавание подозрительных или украденных транспортных средств;
- программы машинного распознавания образов, способные, в том числе в толпе, выделять и распознавать лиц, находящихся в розыске либо подозреваемых полицией в совершении преступлений (не только по полному, но и по частичному изображению);
- программы распознавания голосов на основе сравнительного анализа с образцами, действующие в режиме реального времени. Предположим, полиции удалось записать голос преступника. Программа, подключенная к оборудованию компании мобильной связи, позволяет прослушивать все разговоры. Если имеет место совпадение образца с аудиофайлом разговора, программа автоматически дает команду поставить телефон на прослушку и одновременно определяет его локацию;
- программы латентно-семантического анализа контента, позволяющие на основе содержательного анализа письменных или аудиотекстов определять психологическое состояние их автора, а также скрытые смыслы, заложенные в сообщениях;
- платформенное решение на основе ИИ, позволяющее собирать, хранить и проводить интеллектуальный анализ информации с целью превентивного выявления слабых сигналов, указывающих на всплеск уличной преступности, неконтролируемые волнения, беспорядки, выступления и акты вандализма;
- биометрические методы, позволяющие проводить идентификацию граждан, распознавать преступников и обнаруживать подозрительное поведение по микромоторике мускулов лица и движениям тела и т.п.;
- патрульные роботы периметра;

- функционирующий на основе ИИ полностью автоматизированный комплекс поиска и анализа контента детской порнографии в сети;
- масштабируемая, открытая цифровая система судебной экспертизы;
- комплексные решения на основе ИИ, обеспечивающие переход от бумажного к электронному полицейскому офису;
- интеллектуальные программы на базе ИИ, позволяющие распознавать аномалии при проведении финансовых транзакций, заключении хозяйственных договоров и т.п., способствующие раскрытию финансовых преступлений;
- специализированные программы распознавания необычных колебаний цен на активы, указывающих на инсайдерскую торговлю или криминальное поведение на финансовых рынках;
- автономные роботы, которые могут производить осмотр особо опасных объектов, включая объекты с наличием взрывчатых, отравляющих веществ и т.п.;
- боты, используемые правоохранительными органами для первичных информационных контактов с гражданами и организациями.

Этика использовании полицией ИИ и роботов

Центральный вопрос, который каждое общество должно разрешить сообразно собственным культурным традициям, стереотипам поведения и нормам жизни, — это ***вопрос о полноте цифрового досье и масштабах наблюдения через видеокамеры и данные «Интернета вещей»***.

Вполне вероятно, что в одних обществах будут установлены критерии, которые окажутся неприемлемы в других. Соответственно, *вопрос об этичности — это вопрос контекста, традиции и культуры*. Единых мировых образцов здесь быть не может. Однако, по мнению участников совещания в ОБСЕ, использование ИИ и робототехники в работе полиции и судей должно соответствовать следующим принципам:

- *справедливости*. Система не должна нарушать базисные права, а именно, презумпцию невиновности, свободу слова и свободу от дискриминации;
- *преемственности*. Любые организационно-технические и программные решения должны соответствовать политическим и культурным особенностям и традициям страны, сложившимся в обществе, формальным и неформальным правилам поведения;

- *прозрачности*. Будучи сложными программно-аппаратными комплексами на основе ИИ, используемыми в правоохранительной и правоприменительной деятельности, универсальные системы ни в коем случае не должны быть «черным ящиком». Их решения должны быть объяснимы и логичны как для пользователей системы, так и для лиц, решение по которым системой выносится. Решения и действия системы должны быть понятны пользователям-людям, включая лиц, в отношении которых действует система, а также лиц, ее эксплуатирующих. Любая выводная информация должна быть интерпретирована в виде текстов, таблиц, графических изображений и понятна людям;
- *пропорциональности*. Вполне вероятно, что правоохранительные платформы на основе ИИ будут использованы в первую очередь для мониторинга, предупреждения и расследования особо крупных, а также высокотехнологичных преступлений. Такие преступления потенциально несут максимальные угрозы и риски для общества. Господствующий ныне принцип расследования преступлений может оказаться слишком дорогим для общества. Единственной возможностью пресечения высокотехнологичной преступности без чрезмерного для общества ущерба, скорее всего, окажется превентивный подход. Соответственно, следует ожидать, что для людей с определенными профессиональными, квалификационными и иными характеристикам в ближайшем будущем превентивный контроль будет на несколько порядков выше, чем по отношению к иным гражданам.

Чтобы минимизировать риски и угрозы, создаваемые использованием ИИ правоохранительными и правоприменительными органами, целесообразно разрабатывать соответствующие законы и внутренние нормативные акты на основе международных этических кодексов и рекомендаций.

Каждое общество, каждая страна должны решить для себя, готовы ли они, например, к использованию сплошных систем видеомониторинга и распознавания лиц, к введению обязательного предоставления информации правоохранительным органам производителями «Интернета вещей» или интернет-провайдерами. Только само общество может ответить на вопрос, до какой степени оно готово отступить от принципа неприкосновенности частной жизни и приватности повседневного поведения для перехода от расследования к профилактике преступлений.

На основе обсуждений полиции всех стран мира предложено обратить особое внимание:

— на пресечение постоянно расширяющейся эксплуатации преступниками ИИ как в первую очередь инструмента кибер-, финансовой и иной высокотехнологичной преступности;

— гораздо более широкое, чем в настоящее время, использование ИИ и гибридного интеллекта для прогнозирования поведения преступников, перехода от расследования к более активной превентивной борьбе с преступностью;

— более широкое использование робототехники при патрулировании и оказании помощи, а также при обеспечении информационной осведомленности полицейских «на земле», экипажей полицейских машин и т.п.;

— необходимость преодоления невысокого уровня компетенций рядовых сотрудников полиции в сфере ИИ;

— более широкое использование такой эффективной формы, как государственно-частные партнерства, для более активного вовлечения бизнес-структур и IT-компаний в решение повседневных проблем полиции, связанных с эффективным использованием ИИ;

— расширение международных контактов, связанных с использованием ИИ, ликвидацию дублирования усилий и бессмысленной траты ресурсов, когда каждая полицейская структура стремится решить задачи в одиночку;

— особую чувствительность общественности к угрозам вмешательства в частную жизнь граждан и недопустимость перехода этических границ правоохранительными органами при практическом использовании ИИ.

Европейский правоохранительный подход к ИИ

Европейским сообществом признается возрастающая роль ИИ, в том числе в сфере правосудия и правоохранительной деятельности. Данному вопросу посвящена ***Европейская хартия использования искусственного интеллекта в судебной и правоохранительной системах, одобренная на 31-м пленарном заседании Европейской комиссии (3–4 декабря 2018 г., Страсбург)***.

В Хартии указывается, что использование ИИ в правоохранительной деятельности поможет повысить уровень раскрываемости преступлений, доказательности направляемых в судебные инстанции обвинительных заключений и обеспечить новый уровень обоснованности судебных решений за счет снижения количества ошибок при их вынесении.

Одним из ключевых направлений использования ИИ является прогноз криминогенной обстановки в конкретном городе или

регионе, также он успешно применяется при прогнозировании индивидуального преступного поведения.

На основе возможностей, связанных с применением новых ИКТ, включая технологии ИИ, происходит усиление роли оперативной аналитики в борьбе с преступностью и формирование нового подхода к полицейской деятельности. Появляется возможность существенного повышения роли ОРД, которая основана на работе с оперативными данными и информацией. Роль полицейской деятельности на основе оперативных данных и информации (далее — ***ПДОДИ***) оценивает ОБСЕ, которая считает, что данная деятельность является ключевым элементом по укреплению безопасности и стабильности на европейском континенте.

Так, в Департаменте по противодействию транснациональным угрозам Секретариата ОБСЕ разработано ***Руководство по полицейской деятельности на основе оперативных данных и информации*** (далее — Руководство). ПДОДИ является современной упреждающей моделью правоохранительной деятельности и альтернативой традиционным формам работы полиции, в основе которых лежит реагирование на уже совершенные правонарушения. Во времена жесткой экономии и бюджетных ограничений ПДОДИ предоставляет руководству правоохранительных органов методы и инструменты для определения приоритетов и выделения соответствующих ресурсов[1].

Основное внимание в ПДОДИ уделяется систематическому сбору и оценке данных и информации посредством четко прописанного аналитического процесса, в результате чего данные становятся стратегическими и рабочими аналитическими продуктами, которые служат основой для принятия обоснованных решений.

ИИ в полиции США

По уровню использования ИИ в правоохранительной сфере Европа, за исключением Великобритании, в целом отстает от США.

В правоохранительных органах США совершенствование программно-аппаратного комплекса ИИ осуществляется по ряду направлений и определяется в каждом конкретном случае тем, кто ставит задачи. Рассмотрим основные из этих направлений.

1. *Глубинное обучение* — обучение методом проб и ошибок, при котором после каждого решения задачи программа сверяет достигнутый результат с идеальным и закрепляет алгоритмическое

[1] Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации. Серия публикаций ДТНУ/ОСВПД (13-е изд.).

решение. В этих целях возможно использовать распределенное глубинное обучение, когда множество обучающихся компьютеров увязаны в единую сеть с центральным сервером. При этом результаты обучения каждого из компьютеров являются достоянием всех участников сети.

2. *Метод генетического программирования*, при котором программирование фактически копирует процесс эволюции. Так, генетический алгоритм на каждом этапе выбирает из каждого поколения программы лучшие варианты решения задачи и определенным образом скрещивает их. Главной проблемой, как отмечают американские специалисты, является затрачиваемое время; решение проблемы — скоростные компьютеры.

3. *Сети с памятью, или немарковские процессы*, где каждое последующее событие зависит от предыдущего. В статистике немарковским процессам соответствует так называемая «байесовская» статистика, при которой значение вероятности на каждом шаге процесса меняется в зависимости от прогноза и факта, полученного на предыдущем шаге. Данная методика активно применяется и развивается в *Facebook Al Research*, *Google*, *DeepMind* и других компаниях. Как отмечают представители ФБР, технологической проблемой на данном направлении является определение длительности памяти для каждого процесса.

4. *Масштабирование малых выборок для глубинного обучения*, т.е. создание минимально необходимых выборок для обучения. Так, благодаря стараниям специалистов *IBM* ожидается появление доступного для программной команды инструмента, позволяющего обучать не только на всем объеме данных, но и на минимально необходимой их выборке, что обеспечивает компромисс между качеством обучения и возможностями компьютеров.

5. *Разработка контекстных программ ИИ*. Например, компания *Kimera System* представила для ФБР программу Nigel, которая способна накапливать знания и реакции с учетом контекста. Nigel получает всю доступную информацию от внешних сенсоров различного характера типа видеокамер или датчиков «Интернета вещей», совмещает ее с числовой, текстовой информацией из баз данных и архивов, интегрирует в единый контекст ситуации. В настоящее время ФБР совместно с *Kimera System* и полицейским управлением г. Остина работают над созданием персонального помощника оперативника нижнего уровня полиции, что станет прорывом в применении ИИ в правоохранительной деятельности.

6. *Использование высокоскоростных квантовых компьютеров*. Скорость компьютера — решающее условие дальнейшего прогресса

программных решений, необходимых для создания полноценного инженерного ИИ.

Важным направлением использования ИИ является розыск преступников, ведение профилактических и оперативных учетов.

Количественное и качественное развитие видеонаблюдения в общественных местах стимулирует разработку программ распознания разыскиваемых преступников в видеопотоке. В основе оперативного отождествления личности заложены общеизвестные биометрические признаки, связанные в основном с изображением лица человека.

В 2014 г. ФБР совместно с исследователями из недавних стартапов создали общеамериканскую визуальную базу всех татуировок, зафиксированных когда-либо на территории США и в других странах мира. С использованием трехмерной графики, метода опорных векторов и нейронных сетей для каждой татуировки были созданы примерно 200 вариантов ее фрагментов, открытых для наблюдения в зависимости от различных положений тела и наличия одежды.

Создание вариантной графической базы позволило использовать ее в качестве фильтра при автоматизированном распознавании образов в потоковом видео, поступающем с городских камер наблюдения. Впервые в истории разыскиваемые преступники опознавались не по чертам лица, характерной походке или особым приметам, а по фрагментам татуировок. С 2016 г. система начала эксплуатироваться в городах Сан-Франциско, Сан-Диего и Миннеаполисе.

Кроме того, ИИ используется при розыске преступников, которые приняли меры маскировки, такие как пластические операции. Так, в полицейские участки и подразделения ФБР различных штатов начал поступать как стандартное оснащение первый софт, созданный специалистами стартапа *Cogninive Computing* — бывшими программистами и разработчиками *IBM*, и высококвалифицированными пластическими хирургами Кливлендского госпиталя.

Программа способна по фотографиям и потоковому видео распознавать людей, подвергавшихся пластическим операциям той или иной глубины, и выдавать варианты их первоначальной внешности. В ходе испытаний в 2015 г. программа успешно распознала по фотографиям факт проведения пластической операции в 97% случаев, в потоковом видео — почти в 90%. В случае успешного распознавания более чем в 80% случаев она позволяла восстановить первоначальную внешность.

Существенно повышают эффективность распознавания разыскиваемых лиц современные методики, связанные с использованием различного рода чипов, что позволяет ИИ не только фиксировать их местонахождение, но и своевременно прогнозировать их возможное криминальное поведение.

Так, в 2015 г. Парламент провинции Квебек (Канада) внес изменение в законодательство и разрешил уникальный эксперимент, связанный с профилактикой индивидуальной преступности рецидивистов. Данным лицам в обмен на условно-досрочное освобождение делалась на теле татуировка, представляющая собой сверхтонкий процессор-индикатор, который меняется раз в пять лет. В результате уровень преступности среди данных лиц в первые месяцы после освобождения оказался в 6 раз меньше, чем среди лиц, освобожденных из мест лишения свободы в обычном порядке.

Вместе с тем, несмотря на хорошее техническое и программное оснащение, громадные информационные массивы, в США пока не произошло решающего перехода от традиционных баз данных преступников к принципиально новым базам, пополняемым в режиме реального времени.

ИИ в правоохранительных органах Китая

Одним из интересных и перспективных направлений в части предупреждения и профилактики преступлений является автоматизированный мониторинг поведения лиц, склонных к противоправному поведению. Так, в 2016 г. власти КНР начали вводить систему оценки граждан по степени их благонадежности на основе ИИ и «больших данных».

В настоящее время в некоторых регионах страны тестируется система, которая позволяет создавать цифровые записи о гражданах. В каждой записи (профиле) будут фиксироваться детали социальной жизни гражданина и его финансовые действия. На этой основе формируется так называемый «рейтинг благонадежности», который для любого китайца будет определять возможность получить доступ к определенным сервисам, включая путешествия, образование, страхование и кредиты. Вероятно, за некоторыми категориями граждан будет установлено более пристальное наблюдение со стороны правоохранительных органов.

В итоге власти Китая планируют уже к концу 2020 г. ввести социальный рейтинг 1 млрд 300 млн своего населения, т.е. кибернетическую систему социального ранжирования граждан с компьютерным вычислением ценности каждого гражданина для общества в зависимости от его социального поведения.

Необходимо отметить, что представители КНР активно организуют на своей базе проведение различных форумов по обсуждению вопросов, связанных с применением ИИ и анализом «больших данных». Так, в г. Гуйян 24–28 июля 2018 г. проходил первый форум полицейского международного сотрудничества в сфере использования «больших данных» с участием представителей Китая и сопредельных стран. Помимо России и Китая в форуме приняли участие делегации еще 12 государств: Афганистана, Бангладеш, Казахстана, Лаоса, Малайзии, Мальдив, Мьянмы, Непала, Пакистана, Филиппин, Таиланда и Вьетнама.

Многочисленная делегация хозяев мероприятия состояла не только из представителей МОБ КНР, руководства и профессорско-преподавательского состава китайских полицейских вузов, но и руководства ведущих китайских IT-компаний.

В ходе форума внимание участников было акцентировано на том, что для анализа «больших данных» должны быть изменены традиционные подходы и реализованы новые технологические возможности, так как обрабатывать их с помощью привычных программных и аппаратных средств нецелесообразно, а в некоторых случаях и невозможно.

В докладах китайских представителей (как полиции, так и IT-компаний) было заявлено о намерении интегрировать в ближайшей перспективе правительственные и ведомственные информационные ресурсы с информационными массивами сети Интернет на базе единого центра обработки данных.

Особое внимание было уделено вопросам модернизации деятельности полиции с учетом современных информационных технологий и телекоммуникаций (ИТТ). В докладах выступающих часто использовался термин «цифровая полиция». Китайские коллеги целенаправленно продвигают среди международного полицейского сообщества образ современного китайского полицейского, широко использующего в своей деятельности последние достижения в сфере ИТТ.

По результатам форума был разработан итоговый документ «Общее понимание», призывающий развивать взаимодействие между правоохранительными органами стран-участниц, создать эффективный механизм международного полицейского сотрудничества, активизировать обмен опытом, новыми идеями и технологиями в области «больших данных».

Интегрированный подход Интерпола к использованию ИИ в работе полиции

Международная организация уголовной полиции — Интерпол начиная с 2018 г. проводит в Инновационном центре Интерпола в Сингапуре ***Глобальные совещания Интерпола-ЮНИКРИ (Института УНП ООН) по искусственному интеллекту для правоохранительных органов***.

Третье ежегодное глобальное собрание, проходившее с 23 по 27 ноября 2020 г., объединило более 600 участников из 80 стран.

Главная задача, которую поставил Интерпол, — это создание на основе технологий ИИ и больших данных ***Безопасной интеллектуальной платформы Интерпола для расширенного криминального анализа***.

Чтобы обеспечить максимальное использование огромного количества глобальных полицейских данных, Интерпол разрабатывает ***INSIGHT, передовую аналитическую платформу***, которая сделает анализ более эффективным и действенным для Интерпола и стран-членов. Эта аналитическая платформа будет использовать новейшие технологии для создания современной основы для аналитиков, офицеров и менеджеров при принятии операционных или стратегических решений.

Будет создана ориентированная на будущее, модульная и гибкая аналитическая платформа, позволяющая в полной мере использовать новые и существующие данные и предоставлять полиции во всем мире достоверную, своевременную и действенную информацию, которая выявляет интересующие объекты, способствует расследованиям и укреплению международного полицейского сотрудничества.

Платформа INSIGHT предоставит своим пользователям мощный набор инструментов для создания и применения передовых аналитических продуктов для поддержки расследований и принятия решений.

Она будет использовать передовую аналитику в области ИИ, обработки естественного языка, распознавания и сопоставления сущностей, машинного обучения и автоматизации процессов для обработки постоянно растущих объемов и разновидностей данных, генерируемых в ходе расследований правоохранительными органами. Платформа всегда будет действовать в рамках руководящих принципов и политик Интерпола в отношении использования данных.

Этот масштабный комплексный проект реализуется в несколько этапов.

Фаза первая (минимальная жизнеспособная платформа) — подготовка в середине 2021 г.

Первый этап разработки платформы INSIGHT был запущен в июне 2020 г. с повышенным уровнем подключенных источников данных, выходных и аналитических данных:

— источники данных — все приоритетные внутренние источники данных Интерпола;

— инструменты и методы INSIGHT — идентификация и извлечение сущностей, перевод, сетевой и географический анализ;

— результат — расширенный операционный и стратегический анализ.

Вторая фаза (улучшенная платформа) — 2021–2023 гг.

Второй этап разработки платформы INSIGHT расширит объем и функциональность, чтобы предоставить странам-членам более глубокий анализ:

— источники данных — дополнительные источники и типы данных;

— инструменты и методы INSIGHT — приборная панель, сканирование веб-страниц и оптическое распознавание символов; пилотный доступ к участвующим национальным центральным бюро Интерпола (НЦБ);

— вывод — расширенная аналитика.

Третья фаза (целевая платформа) — 2023–2025 гг.

На заключительном этапе платформа выйдет на полную мощность, включая все внутренние и внешние источники данных и передовые технические системы, чтобы предлагать аналитические продукты высочайшего качества:

— источники данных — все внутренние источники, внешние источники, такие как коммерческие базы данных и т.д.;

— инструменты и методы INSIGHT — визуальное, видео-, аудиораспознавание, сопоставление лиц и биоданных;

— вывод — ***расширенная и предиктивная аналитика***.

В конечном счете новая платформа INSIGHT будет означать, что Интерпол предоставляет своим странам-членам лучшую поддержку для их расследований в мире, где преступная деятельность пересекает границы, преодолевает разрыв между физическим и цифровым миром, и они сами могут воспользоваться преимуществами передовых технологий.

Enter I-Familia — еще одна новаторская база данных Интерпола, основанная на ИИ, официально запущенная в июне 2021 г.

В ней применяются передовые научные исследования и используются ДНК родственников для идентификации неопознанных

человеческих останков или людей, пропавших без вести по всему миру.

Профили ДНК членов семьи можно сравнить с профилями ДНК неопознанного тела или человеческих останков с помощью ***сопоставления ДНК***. Этот метод часто используется, когда прямой образец у пропавшего без вести — из предыдущего медицинского образца или личного предмета, такого как зубная щетка, — недоступен.

Однако для подтверждения совпадения требуются сложные вычисления, потому что биологические родственники имеют разный процент ДНК. Эта сложность усугубляется на международном уровне из-за генетических различий среди популяций по всему миру.

I-Familia — это первая глобальная база данных, которая автоматически учитывает такие различия, не требуя знания генетической родословной пропавшего без вести человека, и предоставляет стандартизированные рекомендации относительно того, что составляет совпадение.

I-Familia открывает новые возможности для стран-членов, которые положительно повлияют на эффективность международных расследований пропавших без вести.

I-Familia — это гуманитарный инструмент, который благодаря глобальному охвату Интерпола открывает новые возможности для выявления пропавших без вести и предоставления семьям ответов.

Чтобы установить связь между пропавшими без вести и делами, связанными с человеческими останками, профили ДНК были представлены 194 странами — участницами Интерпола.

I-Familia состоит из трех компонентов:

- специальная глобальная база данных для хранения профилей ДНК, предоставленных родственниками, отдельно от любых криминальных данных;
- программное обеспечение для сопоставления ДНК Bonaparte, разработанное голландской компанией *Smart Research*;
- руководства по интерпретации, разработанные Интерполом, для эффективного выявления потенциальных совпадений и сообщения о них.

В технологии Бонапарта использованы передовые статистические алгоритмы ИИ для вычисления вероятности совпадения по сравнению с таблицей интерпретации. Это мощное программное обеспечение может выполнять миллионы вычислений за короткий промежуток времени. Затем результат интерпретируется судебными экспертами по ДНК в Генеральном секретариате Интерпола.

Обработка данных ДНК через Интерпол осуществляется через защищенные каналы связи и в соответствии с жесткими правилами защиты данных Организации, а также политикой Интерпола по использованию семейных профилей ДНК пропавших без вести лиц для установления родства.

Члены семьи должны дать согласие на использование их данных для международного поиска.

В случае совпадения уведомления отправляются в страны, предоставившие профиль ДНК от неопознанного тела и от семьи соответственно. Затем могут быть выполнены дополнительные проверки (например, стоматологических записей и личных вещей) для подтверждения потенциального совпадения.

Использование полицией ИИ как инструмента контроля населения в период пандемии COVID-19

Цифровые технологии, включая ИИ, являются важными инструментами для содействия полицией принятию скоординированных ответных мер в связи с пандемией COVID-19 в целях *обеспечения эпидемиологической безопасности*.

Пример Сингапура в борьбе с эпидемическими рисками при поддержке технологий, безусловно, является уникальным и трудным для экспорта из-за общественного признания ограничительных мер безопасности: издание приказа об изоляции населения, подвергающегося риску, проверка соблюдения мер с помощью мобильного телефона и геолокации, выборочные домашние проверки.

ИИ достаточно широко использовался в поддержку такой политики массового наблюдения, как в Китае, где устройства применялись для измерения температуры и распознавания людей или для *оснащения представителей полиции «умными» шлемами*, способными выявлять людей с высокой температурой тела. Устройства распознавания лиц, однако, столкнулись с трудностями из-за ношения хирургических масок. Это привело к тому, что одна компания попыталась обойти эту трудность, так как многие службы в Китае теперь полагаются на данную технологию, в том числе полиция и государственные службы надзора.

В Израиле был разработан план использования индивидуального наблюдения по телефону, чтобы предупреждать пользователей об опасности контакта с людьми, которые потенциально могут быть носителями вируса.

В Южной Корее предупреждение передается органам здравоохранения, когда люди не соблюдают период изоляции, например

находятся в людных местах, таких как общественный транспорт или торговый центр.

На Тайване инфицированным лицам выдается мобильный телефон и записывается их местоположение по данным GPS, с тем чтобы полиция могла отслеживать их передвижения и следить за тем, чтобы они не удалялись от места изоляции.

В Италии компания также разработала приложение для смартфона, с помощью которого можно проследить маршрут зараженного вирусом человека и предупредить людей, контактирующих с ним. По словам разработчика, конфиденциальность будет гарантирована, так как приложение не будет раскрывать телефонные номера или личные данные. В Ломбардии телефонные операторы предоставили данные о передвижении мобильных телефонов с одного терминала на другой.

Правительство США обратилось к этим IT-компаниям с просьбой предоставить доступ к агрегированным и анонимным данным, особенно в отношении мобильных телефонов, для борьбы с распространением вируса. Однако компании проявляют осторожность в связи с юридическим риском и возможностью нанесения ущерба имиджу.

В социальных сетях и интернете участились попытки дезинформации. Идет ли речь о самом вирусе, о способах его распространения или о средствах борьбы с его последствиями, распространяются многочисленные слухи. ИИ — это технология, уже используемая с некоторой эффективностью платформами для борьбы с неподходящим контентом.

9 марта 2020 г. ЮНИСЕФ принял заявление о дезинформации о коронавирусе, в котором Организация заявляет о своем намерении «активно принимать меры по предоставлению точной информации о вирусе, сотрудничая со Всемирной организацией здравоохранения, государственными органами и такими онлайн-партнерами, как *Facebook*, *Instagram*, *LinkedIn* и *TikTok*, для обеспечения доступности точной информации и советов, а также принимая меры по информированию общественности в случае появления неточной информации». Предусматривается также введение ограничительных мер в государствах — членах Совета Европы во избежание разжигания обеспокоенности общественности. Тем не менее Комитет экспертов Совета Европы по медиасреде и реформе СМИ (MSI-REF) в заявлении от 21 марта 2020 г. подчеркнул, что «кризисная ситуация не должна использоваться в качестве предлога для ограничения доступа общественности к информации».

Многократное использование также иллюстрирует пределы того, что в настоящее время может быть достигнуто благодаря этой технологии. Следует напомнить, что ст. 11 Европейской социальной хартии (ратифицированной 34 из 47 государств — членов Совета Европы) устанавливает право на охрану здоровья, которое обязывает подписавшие документ стороны «принять, непосредственно или в сотрудничестве с государственными или частными организациями соответствующие меры, направленные, в частности, на: 1) устранение, насколько это возможно, причин плохого состояния здоровья; 2) предоставление услуг консультационного и просветительского характера, направленных на укрепление здоровья и здорового образа жизни и на развитие чувства личной ответственности за свое здоровье; 3) предотвращение, насколько это возможно, эпидемических, эндемических и других болезней, а также несчастных случаев».

Наконец, должна быть возможность оценить принятые чрезвычайные меры по окончании кризиса, с тем чтобы определить преимущества и проблемы, появившиеся при использовании цифровых инструментов и искусственного интеллекта. В частности, ***временные меры по контролю и массовому мониторингу населения с помощью этой технологии не должны считаться тривиальными и не должны стать постоянными***.

И европейский, и американский подходы заключаются в том, что ***стандарты, касающиеся защиты данных, должны по-прежнему применяться в полном объеме и при любых обстоятельствах: будь то использование биометрических данных, геолокация, распознавание лиц или использование данных о здоровье***.

Принципы и перспективы использования технологий ИИ в оперативно-розыскной деятельности органов внутренних дел Российской Федерации

Примерный перечень принципов использования технологий ИИ в деятельности оперативных подразделений МВД России может быть сформулирован следующим образом.

1. *Использование технологий ИИ исключительно в целях решения задач ОРД ОВД, предусмотренных законодательством*. С учетом возрастающего потенциала современных технологий важно создать условия для минимизации возможности каких-либо злоупотреблений и попыток использовать ИИ не по назначению.

2. *Важное значение взаимодействия с научным сообществом, «стартапами» и технологическими компаниями, как государ-*

ственными, так и работающими в частном секторе. Следует отметить, что именно «стартапы»[1] преимущественно обеспечивают развитие ИИ. Одного лишь диалога с государственными институтами в этом вопросе будет недостаточно. Чтобы добиться максимального эффекта, пользователи технологий ИИ должны на всех этапах сотрудничать с его разработчиками, активно взаимодействовать со «стартапами» и направлять свои усилия на продвижение инноваций в этой области.

3. *Исключение какой-либо дискриминации при принятии решений*. Дискриминация — это широкомасштабная проблема, которая проявляется в самых различных формах и актуальна для огромного количества государственных институтов и частных организаций. Эпоха повсеместного использования технологий ИИ приведет к трансформации этой проблемы в так называемую «алгоритмическую» дискриминацию. Несмотря на то, что в настоящее время превалирует общая тенденция считать решения, принимаемые алгоритмами, свободными от каких-либо недостатков и, следовательно, правильными, реальность такова, что на их качество влияют как специалисты (инженеры-программисты), создавшие алгоритмы, так и исходные данные, которые ими используются. В результате алгоритмы будут неизбежно заимствовать предубеждения своих создателей и те систематические ошибки, которые могут быть заложены (с умыслом либо непреднамеренно) в используемых данных.

Для такой специфической области социальной практики, как ОРД, обозначенная проблема приобретает особое звучание, поскольку юридические последствия дискриминационных решений в отношении конкретных лиц — объектов проведения ОРМ связаны с нарушением фундаментальных конституционных прав и свобод человека и гражданина. При этом в отдельных случаях нанесенный

[1] Стартапом считается фирма или интернет-проект, характеризующийся амбициозной и инновационной идеей или перспективным продуктом. Понятие «стартап» сегодня применяется во всех сферах деятельности, однако больше он распространен в сети Интернет и IT-индустрии. Классический «стартап» в современных условиях, как правило, включает четыре ключевых субъекта (участника): «хакер» (разрабатывает необходимое программное обеспечение), «хипстер» (занимается техническим оформлением разработанного программного продукта), «хастлер» (отвечает непосредственно за эксплуатацию продукта), аналитик (занимается мониторингом информационного пространства, сбором сведений, важных для успешного функционирования «стартапа») (см., например: *Назаренко В.А., Бочкова Е.В.* Стартапы: сущность и основные составляющие развития // Научно-методический электронный журнал «Концепт». 2016. Т. 11. С. 3946–3950. URL: http//e-koncept.ru/2016/86828.htm).

такими нарушениями ущерб может иметь необратимый характер для лица, права которого нарушены.

4. *Прозрачность механизмов принятия решений и подотчетность ответственных лиц.* Алгоритмическое принятие решений (особенно в процессе подготовки и проведения ОРМ, определения порядка использования их результатов) проблематично не только из-за предубеждений, но и из-за своей непрозрачности. Нередко бывают ситуации, когда даже сами люди, создавшие алгоритм, из-за его сложности иногда не знают, каким образом он пришел к тому или иному решению. Эту особенность зачастую описывают как «черный ящик» ИИ: мы знаем вход и выход, но не знаем сам путь из точки А в точку Б. Уже звучат призывы к тому, чтобы сделать работу ИИ более прозрачной и понятной, и это один из главных принципов, на которых Европейский союз сосредоточил свой подход к вопросу его развития[1].

5. *Максимальная защита оперативно значимых сведений, полученных в результате использования технологий ИИ.* В последние несколько лет защите данных уделяется все более пристальное внимание. Технологии ИИ, с одной стороны, упрощают эту задачу, с другой — закономерно добавляют сложности, поскольку системы ИИ требуют огромного количества данных. Необходимо, чтобы люди знали об этом, а также о том, каким образом их персональные данные (биометрические и установочные данные, различного рода контрольная информация) могут быть использованы, иногда даже им в ущерб.

6. *Необходимость адаптации оперативно-розыскного законодательства к новым условиям активного использования технологий ИИ.* Активное использование технологий ИИ, безусловно, приведет к изменениям в законодательстве. Существующие законы будут обновляться для обеспечения отражения фактических изменений, связанных с расширением применения ИИ, а для заполнения возможных пробелов будут создаваться новые.

Применительно к сфере ОРД уже назрела потребность в изменении ряда законодательных положений с целью повышения эффективности проводимых ОРМ, в первую очередь направленных на выявление, предупреждение, пресечение и раскрытие преступлений, совершаемых с использованием ИКТ. В частности, эти изменения касаются сроков исполнения запросов оперативных подраз-

[1] См., например: Сбер представил перспективы искусственного интеллекта // Журнал ПЛАС: новости, технологии. 2020. 19 нояб. URL: https://plusworld.ru/daily/tehnologii/sber-predstavil-perspektivy-iskusstvennogo-intellekta/ (дата обращения: 20.08.2021).

делений ОВД, упрощения порядка санкционирования проведения отдельных видов ОРМ, расширения полномочий оперативных руководителей и сотрудников по использованию современных достижений науки и техники в процессе оперативно-служебной деятельности и т.д.

7. *Формирование и постоянное повышение уровня профессиональной подготовки и квалификации сотрудников оперативных подразделений ОВД, что позволяет максимально эффективно и безопасно использовать технологии ИИ в повседневной служебной деятельности*. Смысл заключается в том, что обладание знаниями в сфере ИКТ и уверенное ориентирование в цифровой (виртуальной) среде постепенно становятся не уделом ограниченного круга специалистов, имеющих соответствующую квалификацию и образование, а непременным условием, позволяющим выполнять свои профессиональные обязанности на должном уровне. Речь, конечно, не о том, чтобы каждый оперативный руководитель и сотрудник стали высококлассными специалистами в области IT-технологий, но увеличение среди личного состава оперативных служб количества уверенных и грамотных пользователей соответствующих компьютерных и иных технических средств, необходимых для предупреждения и раскрытия преступлений в условиях всеобщей цифровизации, — вполне достижимая задача.

Среди проблем, связанных с использованием технологий ИИ в деятельности ОВД, справедливо выделяются следующие:

- невозможность полного соблюдения требований по защите персональных данных при их использовании для обучения систем ИИ;
- отсутствие правосубъектности ИИ и соответствующего статуса принимаемых на основе его технологий решений;
- низкая надежность решений, вырабатываемых системами ИИ, и невозможность в ряде случаев полного обоснования таких решений.

Для обеспечения успешного внедрения и дальнейшего использования технологий ИИ в системе МВД России необходимо разработать и принять:

- нормативный правовой акт, регламентирующий использование технологий ИИ субъектами их применения по направлениям деятельности подразделений системы МВД России;
- административные регламенты (в том числе: использования результатов работы ИИ для принятия процессуальных и управленческих решений; организации обучения систем ИИ);

- ведомственные стандарты (в том числе: понятия и термины; безопасность и прозрачность технологий ИИ).

Качественное повышение эффективности деятельности ОВД на основе технологий ИИ возможно лишь при их массовом применении как средства коллективного или индивидуального пользования. Практически данный подход в ближайшей перспективе может быть реализован на основе специализированных сервисов в ИСОД МВД России, а также сервисов в сети Интернет для исполнения внешних по отношению в системе МВД России функций.

Во всех субъектах применения технологий ИИ в МВД России предполагается создать центры компетенции на базе образовательных, научных и иных подразделений и отдельных организаций. Их основной задачей является научно-методическое обеспечение внедрения и эксплуатации технологий ИИ на основе выполнения следующих функций:

— обучение и переподготовка личного состава, непосредственно применяющего, эксплуатирующего технологии ИИ, а также руководителей применяющих и эксплуатирующих их подразделений;

— поддержание контактов с разработчиками применяемых технологий ИИ, носителями необходимых знаний, научными и иными организациями по вопросам применения эксплуатируемых и перспективных технологий ИИ;

— консультативная, а при необходимости практическая помощь органам по вопросам использования технологий ИИ в режиме реального времени.

Из совокупности имеющихся и перспективных технологий ИИ в интересах обеспечения оперативно-розыскного противодействия преступности могут быть использованы:

- алгоритмы ИИ, нацеленные на распознавание подозрительных или угнанных, похищенных транспортных средств, в том числе тех, водители которых скрылись с места происшествия;
- системы распознавания образов, способные в том числе выделять и распознавать в транспортных потоках и скоплениях людей лиц, находящихся в розыске либо подозреваемых в совершении преступлений, как по полному, так и по частичному изображению;
- системы распознавания (идентификации) человеческой речи, действующие в режиме реального времени;
- системы контентного и семантического анализа текстов и человеческой речи, в том числе для оценки психологического состояния их автора, а также скрытых смыслов, заложенных в сообщениях;

- комплексные решения, позволяющие собирать, хранить и проводить интеллектуальный анализ разнородной информации с целью превентивного выявления слабых сигналов, в том числе указывающих на возможный всплеск преступности;
- биометрические системы, позволяющие в реальном масштабе времени проводить идентификацию граждан по отпечаткам пальцев и ладоней рук, изображений лиц и радужной оболочке глаз, татуировкам, шрамам, голосовым файлам;
- автоматизированные системы поиска и анализа контента сексуальной эксплуатации несовершеннолетних в сети Интернет;
- комплексные решения, обеспечивающие переход от бумажного документооборота к автоматизированному рабочему месту сотрудника ОВД;
- технологии ИИ для автономных роботов и робототехнических комплексов, обеспечивающих решение задач ОВД, в том числе осмотр мест происшествия, особо опасных объектов, включая объекты с наличием взрывчатых, отравляющих веществ и т.п.;
- системы поддержки планирования и принятия управленческих решений, в том числе для определения оптимальных вариантов проведения оперативно-профилактических мероприятий и ОРМ;
- системы предиктивной аналитики, обеспечивающие поиск и получение данных для прогнозирования будущих криминальных событий;
- создание киберфизических систем, основанных на интеграции вычислительных и физических синергетически увязанных ресурсов.

Применительно к сфере ОРД ОВД важно отметить, что развитие новых ИТТ позволяет коренным образом изменить организацию ведения профилактических и оперативных учетов. В данном контексте все чаще применяется термин «цифровое досье» (электронное досье, цифровой профиль и пр.).

В начале 2000-х гг. профессор Университета Дж. Вашингтона Д. Солв впервые ввел в оборот термин ***«цифровое досье»***[1], которое предполагает пассивное наблюдение и сбор о человеке цифровых данных, характеризующих каждый аспект его жизни, начиная от маршрута и продолжительности ежедневных прогулок вплоть до предпочтений в еде и страсти к путешествиям. По мнению

[1] См.: *Овчинский В.С., Ларина Е.С.* Искусственный интеллект. Большие данные. Преступность (Коллекция Изборского клуба). М.: Книжный мир, 2018.

Д. Солва, не только правительство, но и корпорации неизбежно придут к составлению обширных цифровых досье на каждого гражданина, максимально насыщая их данными.

Логично, что первыми на этот путь должны были встать правоохранительные органы. Однако в реальности монополистами цифровых досье на граждан по всему миру стали поисковики типа *Google*, социальные сети типа *Facebook*, торговые платформы типа *Amazon*, *eBay* и брокеры данных. При этом полицейские досье по своей структуре, оперативности пополнения и форме хранения в основном повторяют картину конца XX в. и несопоставимы с гигантскими бизнес-хранилищами корпораций.

Одной из проблем использования ИИ в правоохранительной деятельности является исключение влияния на применяемые алгоритмы случайных или специально подобранных данных, которые могут привести к дискриминационным решениям. Кроме того, проблемой является отсутствие ясности для должностных лиц, принимающих решения, в следующих вопросах: на основании каких именно факторов и с какой значимостью каждого из них ИИ относит человека или объект к одной совокупности, а не к другой?

МВД России намерено активно использовать технологии ИИ в специализированном программном обеспечении, которое призвано в автоматизированном режиме ***выявлять признаки серийных (взаимосвязанных) преступлений, а также определять внешние анатомические признаки преступников (цвет глаз и волос, форму лица и головы) по полученному с мест совершения преступлений биоматериалу, например следам крови***.

МВД России обратилось к бизнес-сообществу за консультативной помощью в составлении технических заданий. Сейчас возможные связи между серийными преступлениями устанавливаются фактически «вручную», однако специализированный софт с использованием технологий ИИ позволит в автоматизированном режиме анализировать описания преступлений, показания свидетелей и другие документы, выявляя в них совпадения (например, место совершения преступления или обнаруженные на нем предметы). Внешность преступника устанавливают, составляя фоторобот, а также по найденным на месте преступления биоматериалу и дактилоскопической информации, но только при наличии соответствующих сведений в банке данных.

За счет реализации проекта МВД рассчитывает повысить эффективность выявления и раскрытия преступлений; составления психофизического портрета преступника и установления личности неопознанных жертв.

В будущем систему можно будет использовать без существенных доработок в деятельности СК России, ФСБ России, ФСИН России и других ведомств, а также экспортировать криминалистические технологии в другие страны.

В перспективе система должна объединить ресурсы дактилоскопической и фоноскопической информации, лабораторий ДНК-анализа, комплексов биометрической идентификации личности и фиксации передвижения транспортных средств, а также систем проверки по оперативно-справочным, розыскным и криминалистическим учетам.

Внедрение системы анализа и поиска закономерностей потребует создания инфраструктуры постоянного (как минимум периодического) централизованного сбора данных о совершенных преступлениях и результатах их расследования. Реализация подобного проекта, учитывая количество, территориальное и структурное распределение подразделений МВД России, равно как и специфику данных, может оказаться гораздо более сложной задачей, чем обработка результатов.

Начать подготовку соответствующих технических заданий МВД России намерено уже в текущем году, а в 2023 г. — приступить к опытно-конструкторским работам по созданию софта, возможно, с привлечением частных IT-компаний.

Таким образом, возможности по выявлению, предупреждению и раскрытию преступлений, которые предоставляют сегодня новые технологии ИИ, являются многообещающими, особенно с учетом крайней перегруженности сотрудников ОВД. Однако, помимо обнадеживающих перспектив, возникает и множество рисков. Будет ли использование новых технологий правоохранительными органами направлено исключительно на борьбу с преступностью, и насколько велик риск различного рода злоупотреблений? Например, необоснованное вмешательство в результате работы алгоритмов машинного обучения в частную жизнь граждан, даже непреднамеренное, многие рассматривают как реальную проблему.

Необходимо отметить некоторые важные моменты, на которые следует обратить внимание в части осмысления передового зарубежного опыта в борьбе с преступностью в информационном обществе с позиции его преломления к российским условиям.

Что касается опыта использования ИИ в деятельности правоохранительных органов, то имеет место тождественность проблем, которые должны быть решены. Среди них можно выделить следующие: создание крупных хранилищ информации; интеграция имеющихся информационных систем и унификация аппаратно-

программного обеспечения; повышение общей квалификации полицейских для обеспечения их готовности работать с технологиями ИИ; привлечение к содействию гражданских специалистов для работы с «большими данными»; развитие системы цифровых досье (профилей), обновляемых и пополняемых в режиме реального времени, и методик автоматизированного мониторинга социальной опасности лиц, состоящих на оперативных и профилактических учетах.

В условиях новой промышленной революции, основанной на применении информационных технологий, во главу угла в сфере борьбы с преступностью поставлен вопрос о формировании ***предиктивной функции полиции*** в качестве основного приоритетного направления ее оперативно-служебной деятельности. Эта тенденция обусловлена острой социальной потребностью развивающегося информационного общества в безопасной и максимально комфортной реализации новых цифровых возможностей во всех сферах жизнедеятельности. В условиях всеобщей цифровизации ущерб, наносимый как отдельными преступниками, так и организованными преступными формированиями, характеризуется огромными финансовыми и ресурсными потерями, поэтому упреждающие меры реагирования закономерно становятся приоритетными.

Организационно-технологической основой реализации предиктивной (предупредительной) деятельности ОВД (полиции) должна стать ***единая оперативно-розыскная информационно-аналитическая система (по аналогии с новой системой Интерпола INSIGHT)***.

Технологии ИИ и методики обработки «больших данных» в процессе эксплуатации этой системы следует использовать эффективно и оптимально, но обязательно с учетом тех рисков, которые выявлены по результатам практической работы российских и зарубежных подразделений.

Данное обстоятельство требует серьезного теоретического осмысления богатого отечественного опыта формирования ***института оперативно-розыскной профилактики*** и использования ***опыта оперативно-розыскной аналитики*** в части возможностей технологий ИИ.

Определенные шаги в этом направлении уже предприняты.

Так, в 2017–2019 гг. по данной тематике сотрудниками ФГКУ «ВНИИ МВД России» подготовлен проект ***Концепции оперативно-аналитического обеспечения оперативных подразделений органов внутренних дел Российской Федерации***. В рамках указанного проекта Концепции выработан и обоснован комплекс

нормативно-правовых и организационно-управленческих мер, направленных на создание и развитие новой организационно-технологической платформы деятельности оперативно-аналитических подразделений ОВД в соответствии с современными реалиями. Эти меры предполагают формирование такой системы противодействия угрозам общественной безопасности в зоне ответственности МВД России, в которой акцент с фиксации совершенных правонарушений и преступлений смещается на упреждающее прогнозирование и проактивную (превентивную) диагностику индивидуального и группового преступного поведения, а также автоматизацию поисковых процессов на основе самосовершенствующихся алгоритмов, методов обработки «больших данных», безопасного программного обеспечения и сервиса.

Две основные проблемы при внедрении ИИ в ОРД

1. Есть мнение, что *внедрение ИИ позволит значительно сократить численность полиции*, как это происходит, например, в банковских структурах. Но, на наш взгляд, следует избегать прямых аналогий. Например, внедрение ИИ в систему видеонаблюдения и расширение этой системы, безусловно, увеличат объем поступающей информации о противоправных проявлениях, которым надо давать уголовно-процессуальную оценку. А это означает, что автоматически потребуется увеличить штат оперативных работников, дознавателей, следователей, экспертов. Уже сейчас требуется подготовка большого числа специалистов новой профессии — аналитиков «больших данных». Поэтому внедрение ИИ вызовет необходимость не сокращения, а увеличения штатной численности полиции.

2. *Различия в этических рекомендациях применения ИИ в полиции и судебной системе*. Во всех недавно принятых международных документах по вопросам использования ИИ в полицейской и судебной деятельности эти рекомендации и ограничения одинаковы как для полиции, так и для судей. Но, на самом деле, здесь возникают серьезные противоречия. Например, в применении принципа прозрачности баз данных для судов и полиции. Если транспарентность судебных баз данных не вызывает сомнения, то в отношении ОРМ имеются серьезные ограничения, связанные с их секретностью и возможными негативными последствиями как для источников информации, так и для потерпевших, подозреваемых и обвиняемых.

ИИ и ОРД в недалеком будущем

Технологии развиваются с такой быстротой и ставят такие вопросы, ответить на которые пока весьма сложно. В том числе и с точки зрения их применения в ОРД.

Так, в правительстве РФ разрабатывают новую ***федеральную программу «Мозг, здоровье, интеллект, инновации»***. Среди прочего она ориентирована на развитие ***технологий «мозг — компьютер»***, позволяющих ***вживлять в мозг человека микрочипы для прямой передачи информации с внешних устройств***. Кроме того, программа предполагает создание ***аватаров*** людей для дистанционного управления транспортом и компьютеров, которые помогают принимать решения.

При Минобрнауки России создана рабочая группа для проработки этой федеральной программы. Проект разработан Российской академией наук совместно с МГУ и одобрен Владимиром Путиным в марте 2021 г. Стоимость программы оценивается в 54 млрд руб., средства на нее планируется выделить из нацпроектов «Наука», «Демография», «Здравоохранение», «Производительность труда и поддержка занятости» и «Цифровая экономика».

Проект предполагает в том числе развитие ***технологий нейроинтерфейсов*** (*brain-computer interface — BCI*). Это набор программно-аппаратных комплексов, позволяющих управлять внешними устройствами (компьютером или экзоскелетом) напрямую с помощью электрических сигналов мозга, которые трансформируются в команды управления при помощи ***технологий ИИ***.

Планируется создание интерфейсов «человек — техника» для управления сложными системами (самолеты, АЭС, автомобили) как непосредственно, так и удаленно, по принципу дистанционного присутствия, аватара. Это позволит людям работать в недоступных местах с высокой радиацией, космосе и т.д. Будут также созданы интерфейсы, обеспечивающие «самостоятельное формирование целей, оценку ситуаций, прогнозирование их развития и принятие решений.

Мировой рынок нейроинтерфейсов в 2019 г. составил 1,2–1,3 млрд долл. До 2027 г. сегмент будет расти в среднем на 15% в год. США за семь лет уже инвестировали в технологии «мозг — компьютер» более 1,2 млрд долл. Планируемый объем вложений составляет 6 млрд долл. В Китае принят *China Brain Project* с финансированием не менее 3 млрд долл.

Технологии «мозг — компьютер» давно разрабатываются в России для диагностики и лечения заболеваний. Например, на людей после перенесенного инсульта надевают специальную ша-

почку с электродами, с которых сигнал передается на экзоскелет: человек посылает на устройство мысль о том, что хочет сжать мячик, и прибор его сжимает. Это помогает быстрее пройти реабилитацию. Через интерфейсы «мозг — компьютер» можно также управлять умным домом.

Но самые передовые интерфейсы, — это те, которые встроены непосредственно в мозг человека. Такие технологии позволяют не только передавать сигнал от носителя, но и направлять данные прямо ему в мозг.

Вот здесь непременно возникнет желание у какого-либо субъекта ОРД ***использовать такие интерфейсы в целях борьбы с преступностью и обеспечения безопасности***. А это влечет за собой огромный объем проблем правового, этического и оперативно-тактического характера.

Раздел III
МЕТОДОЛОГИЧЕСКИЕ ПРОБЛЕМЫ ТЕОРИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ В ЦИФРОВОМ МИРЕ

А.Л. Осипенко

Цифровизация общества и виртуализация реальности: усложнение вызовов и расширение перспектив оперативно-розыскной деятельности

Мы живем в мире, в котором все больше
и больше информации и все меньше и меньше смысла.
Ж. Бодрийяр[1]

Тезис, приведенный в качестве эпиграфа, сформулирован философом Ж. Бодрийяром еще в прошлом веке, однако актуальность его в последнее время только усиливается. Под влиянием информационных технологий существенно меняются многие параметры среды обитания человека. Лавинообразно нарастающие практически неконтролируемые потоки информации становятся одной из причин резкого повышения степени необъяснимости и даже бессмысленности отдельных событий, недоверия граждан к предлагаемым смыслам. Современные исследователи сетуют на то, что «объем информации растет в геометрической прогрессии, а качественный контент съеживается как шагреневая кожа, уходит в небытие»[2]. Непонимание происходящего влечет рост тревожности в обществе: люди опасаются неожиданных и малопонятных угроз, возникают самые абсурдные конспирологические теории, усиливаются депрессивные настроения. Все это получает мощное отражение в трансформации криминогенных факторов.

Среди процессов, наиболее зримо влияющих на социальные изменения в последнее время, особо выделим два взаимосвязанных тренда — *цифровизацию* и *виртуализацию* окружающей нас реальности.

Цифровизация определяется как глобальный процесс масштабного внедрения цифровых технологий во все сферы общественной жизни (промышленность, экономику, образование, науку, здравоохранение, обеспечение общественной безопасности и др.).

[1] *Бодрийяр Ж.* Симулякры и симуляции. М.: Постум, 2015.

[2] *Чернышов А.Г.* Искусственный интеллект в качестве новой религии и идеологии цифровых данных // Власть. 2019. Т. 27. № 2. С. 76–83.

Она основана на интенсивном развитии информационных технологий и поддерживается государством в качестве основного драйвера ускоренного перехода к информационному обществу. В Российской Федерации разработан комплекс программных документов, направленных на формирование условий для эффективного осуществления цифровизации. С 2019 г. реализуются Государственная программа «Научно-технологическое развитие Российской Федерации»[1] и «Национальная стратегия развития искусственного интеллекта до 2030 года»[2]. В них в качестве основных технологий, обеспечивающих достижение намеченных целей, названы: квантовые технологии, анализ больших данных, нейротехнологии, «Интернет вещей», облачные технологии, компоненты робототехники, технологии виртуальной и дополненной реальности. Особое место отводится *технологиям ИИ*, обеспечивающим решение сложных задач, требующих интеллектуальных усилий (принятие решений в изменяющихся условиях; распознавание образов, символов и речи; перевод с одного языка на другой и т.п.). Важной составляющей функционирования этих технологий является машинное обучение[3]. ИИ может восприниматься в качестве примера симуляции, представляющей собой даже не копию естественного интеллекта, а копию воображаемой (виртуальной) модели интеллекта. Это «самобытное образование со своей онтологией, в которой тождество и различие, реальность и виртуальность, упорядоченность и хаос, контролируемость и непредсказуемость образуют объект, новый даже для его создателей»[4].

В свою очередь, *виртуализация реальности* является менее очевидным трендом современности, однако, как и цифровизация, оказывает существенное влияние на многие общественные процессы, в том числе, как будет показано ниже, на изменение условий осуществления и характера ОРД.

---

1 Постановление Правительства РФ от 29 марта 2019 г. № 377.

2 Указ Президента РФ от 10 октября 2019 г. № 490.

3 Оно обеспечивает последовательное повышение эффективности достижения конкретной цели за счет применения алгоритмов, оценивающих результаты, получаемые на основе множества исходных данных, и выявляющих с использованием статистических методов определенные закономерности и оптимальные наборы действий, которые могут быть использованы при последующем решении поставленных задач.

4 *Игнатов А.Н.* Противодействие преступности: симулякры и симуляции // Ученые записки Крымского федерального университета им. В.И. Вернадского. Юридические науки. 2020. Т. 6 (72). № 1. С. 215–226.

Виртуализация реальности не является порождением нашего времени. Искаженное либо скорректированное представление об отдельных сторонах действительности, их моделирование имели место и ранее[1]. Однако именно с развитием информационных технологий и переходом на их основе к тотальной цифровизации общества можно говорить о резкой активизации процессов виртуализации[2]. Исследователи отмечают, что «информационное пространство сегодняшнего общества значительно отличается от того, что окружало человека в 70–80-х гг. XX в., главным образом тем, что широкое распространение получили технологии виртуальной реальности... Глубина проникновения виртуальности в социальную и индивидуальную жизнь позволяет говорить о "виртуализации" общества»[3]. Понятие «виртуализация» широко используется «для характеристики новых экономических, политических и других феноменов социальной реальности. ...Вся социальная и культурная жизнь начинает виртуализироваться, то есть перемещаться в поле виртуальных коммуникаций, которые носят символический характер»[4].

Границы, отделяющие виртуальный мир от реального, постепенно размываются, виртуальные явления и события оказывают все более заметное влияние на реальную жизнь. Еще Ж. Бодрийяр

---

1 Так, по мнению А.А. Бартова, «задолго до того, как западная цивилизация посредством компьютерной техники и других массовых средств коммуникации начала создавать гиперреалистические объекты (виртуальную действительность), эта задача уже решалась советской идеологией, прессой, статистикой». Например, «количественные и качественные цифры переписи населения представляли собой виртуальную действительность». *Бартов А.А.* Философия современного искусства: создание гиперреальности и деконструкция культуры // Нева. 2004. № 11.

2 Некоторыми философами вполне серьезно обсуждается даже гипотеза о том, что вся наша реальность является компьютерной симуляцией, которая поддерживается мощной компьютерной программой. См.: *Bostrom N.* Are You Living in a Computer Simulation? // Philosophical Quarterly. 2003. Vol. 53. № 211. P. 243–255. URL: https://www.simulation-argument.com/simulation.pdf (дата обращения: 20.08.2021); *Chalmers D.J.* The Matrix as metaphysics. 2005 // David Chalmers. URL: http://consc.net/papers/matrix.pdf (дата обращения: 20.08.2021).

3 *Емелин В.А.* Симулякры и технологии виртуализации в информационном обществе // Национальный психологический журнал. 2016. № 3 (23). С. 86–97.

4 *Радевич Е.В.* Глобальное информационное пространство современности: естественное vs виртуальное // Проблема соотношения естественного и социального в обществе и человеке. 2020. № 11. С. 89–95.

связывал эти процессы с переходом общества в эпоху гиперреальности[1], «в которой картинка важнее содержания, связь между предметами, явлениями и их знаками нарушена». В его представлении мощный поток информации размывает или даже уничтожает реальность, подменяя ее огромным количеством копий и симулякров[2]. Погружаясь в условия гиперреальности, человек оказывается оторванным от реального мира, воспринимает не истинную действительность, а ее искусственную подмену.

В то же время «виртуальная реальность в современной ее форме влияет не только на личность, но и на всю социальную систему, преобразуя последнюю»[3]. В повседневный оборот уверенно вошли термины «виртуальное пространство», «виртуальное обучение», «виртуальное общение», «виртуальная валюта», «виртуальная занятость» и др. Появилось даже понятие «виртуальные ценности», и, по оценкам социологов, виртуализация системы ценностей современного общества «тяжело переживается обычным человеком, особенно молодежью, компенсируется различного рода маргинальными, виртуальными или фантастическими формами идентификации: молодежными субкультурами, сектами, религиозным или псевдорелигиозным фундаментализмом, анархизмом»[4].

Особый интерес с позиций ОРД представляет *виртуализация информационного пространства* современного общества. Информационное пространство — это пространство, в котором создается, перемещается и потребляется информация[5]. В информационном

---

1 В философии постмодернизма термин «гиперреальность» определяет феномен симуляции действительности, связанный с неспособностью сознания отличить реальное от нереального или виртуального.

2 Один из базовых терминов философии постмодернизма «симулякр» обозначает копию чего-либо (объекты, явления, смыслы, события), что в действительности не существует. Симулякр выступает основой симуляции реальности — искаженного отображения реальных либо несуществовавших событий.

3 *Смолиговец О.С.* Субъектные основы виртуализации социальной реальности в информационном обществе // Изв. Сарат. ун-та. Сер. Философия. Психология. Педагогика. 2019. Т. 19. Вып. 2. С. 166–170.

4 *Емелин В.А.* Куда нас приведет болезненная степень бессмысленности: симулякры постнормального мира // Независимая газета. URL: https://www.ng.ru/scenario/2019-09-23/9_12_7683_simulakr.html (дата обращения: 20.08.2021).

5 См.: *Проскурин С.А.* Геополитическое измерение глобального информационного пространства // Геополитика: учебник / под общ. ред. В.А. Михайлова. М.: Изд-во РАГС, 2007.

пространстве может быть выделено *информационное поле*[1], *содержащее оперативно значимую информацию*, законы формирования и функционирования которого под влиянием рассматриваемых процессов заметно меняются. Информационное пространство виртуализируется особым образом: оно постоянно расширяется, усложняется, становится неоднородным, наполненным противоречивыми сведениями. Исследователи отмечают, что современное информационно-коммуникативное пространство «достаточно сильно отличается от всех ранее известных человеку и характеризуется нелинейностью взаимодействия людей, принципиальной детерриторизацией и появлением особой сетевой культуры в пространстве Интернета»[2].

Распространенность в глобальной сети анонимных информационных источников, отсутствие ответственности авторов за достоверность размещаемой информации влекут утрату доверия практически к любым поступающим сведениям. Совершенствуются технологии дезинформации, с их применением любая информация может быть легко сфальсифицирована или искажена. Развиваются и информационные технологии управления обществом, формирования общественного сознания, конструирования особого восприятия реальности. Все эти факторы не могут не учитываться субъектами ОРД при добывании оперативно значимой информации.

В качестве особого объекта, связывающего информационное и физическое пространство, может рассматриваться *киберпространство* — виртуальная среда реализации общественных отношений, образованная в результате сложных взаимодействий пользователей сети Интернет с техническими устройствами ее инфраструктуры при наполнении и использовании информационных ресурсов. В нем (безусловно, с явной спецификой) постоянно образуются виртуальные (цифровые) следы практически любой активности пользователей, причем их объем в большинстве случаев внушителен.

Киберпространство «стало новой средой жизнедеятельности человека как субъекта киберсоциализации... обеспечивает отличные от условий реальной жизнедеятельности возможности коммуни-

---

[1] См.: *Ожерельева Т.А.* Об отношении понятий информационное пространство, информационное поле, информационная среда и семантическое окружение // Международный журнал прикладных и фундаментальных исследований. 2014. № 10. С. 21–24.

[2] *Радевич Е.В.* Глобальное информационное пространство современности: естественное vs виртуальное // Проблема соотношения естественного и социального в обществе и человеке. 2020. № 11. С. 89–95.

кации, принадлежности человека к определенным социальным категориям, референтной группе и относительно безопасное экспериментирование с идентичностью»[3]. Построение его пользователями собственных виртуальных образов, которые по желанию владельцев можно наделить любыми отсутствующими на самом деле атрибутами нереальной жизни, постепенно уводит их от адекватного восприятия окружающей действительности, стирает границы между правдой и вымыслом, подменяет реальные ценности мнимыми, а затем влечет и неприятие отдельных социальных норм. Не случайно в виртуальных коммуникационных средах социальных сетей получают распространение такие явления, как склонение к суициду или потреблению наркотических веществ, вовлечение в экстремистскую деятельность, в антиобщественные движения (такие, например, как АУЕ), в террористические организации.

Рассмотренные выше явления и процессы, обусловленные расширением спектра информационных технологий и интенсивным обновлением технологических решений, не могут оставаться без внимания со стороны оперативно-розыскной науки[4]. Важно с ее позиций выработать системное представление о новой цифровой и виртуализирующейся реальности, в которой должны решаться задачи ОРД. Специалисты отмечают, что к настоящему моменту «целостная теория этой реальности отсутствует... Поэтому главная задача современных исследований — изучение новой реальности и обобщение имеющихся фрагментарных разработок»[5].

На наш взгляд, исследование особенностей осуществления ОРД в особой среде важно предварить анализом влияния специфики этой среды на характерные для нее противоправные проявления, которые могут рассматриваться в качестве существенных *криминальных угроз* безопасности киберпространства и, соответственно, новых *вызовов* ОРД.

1. Прежде всего, следует выделить основную тенденцию — активное освоение новой виртуальной среды — киберпространства —

---

[3] *Емелин В.А.* Симулякры и технологии виртуализации в информационном обществе // Национальный психологический журнал. 2016. № 3 (23). С. 86–97.

[4] См.: *Осипенко А.Л.* Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // Научный вестник Омской академии МВД России. 2019. № 4. С. 38–46.

[5] *Делягин М.* Некоторые объективные тенденции глобальной трансформации человечества // Делягин.ру. URL: https://delyagin.ru/articles/187-pozitsija/56788-nekotorye-ob-ektivnye-tendentsii-global-noy-transformatsii-chelovechestva (дата обращения: 20.08.2021).

преступностью, которая для достижения своих целей использует все его особые качества (такие, как наднациональный экстерриториальный характер, широкое распространение средств анонимизации, возможность применения дистанционных, в том числе трансграничных, способов совершения преступлений и др.). В киберпространстве сформировался особый вид криминальных проявлений, объединяемых понятием «киберпреступность», с постоянно нарастающими масштабами наносимого ущерба и количества жертв, с расширяющимся составом участвующих лиц[1]. Процесс *криминализации киберпространства* протекает стремительно, с постоянным поиском преступниками новых уязвимых мест и расширением спектра применяемых ими методов, которые становятся все более изощренными[2].

Этот процесс характеризуется двумя тенденциями. С одной стороны, усиливается организованность самой киберпреступности, а с другой — для решения криминальных задач ее все чаще привлекает традиционная организованная преступность. Особую проблему образует применение криминалом информационных технологий, при поддержке которых возможны разработка и внедрение новых схем криминальной деятельности, не выявляемых традиционными средствами. В результате широкого применения схемы «киберпреступление как услуга» происходит повышение доступности криминальных кибертехнологий.

Изменения касаются и принципов функционирования преступных сообществ: на смену хакерам-одиночкам, движимым главным образом любознательностью и идеалами свободного доступа к любой информации, пришли мощные организованные группы корыстных преступников (такие, как *MoneyTaker*, *Cobalt*, *Lazarus* и др.), которые действуют продолжительное время и периодически совершают масштабные акции.

---

[1] Следует понимать, что противоправные действия в виртуальном пространстве влекут реальные негативные последствия. Отдельные исследователи оценивают как вполне вероятную возможность совершения преступлений непосредственно в виртуальных средах. См.: *Дремлюга Р.И., Крипакова А.В.* Преступления в виртуальной реальности: миф или реальность? // Актуальные проблемы российского права. 2019. № 3. С. 161–169.

[2] Не случайно в опубликованной в апреле 2021 г. Стратегии ЕС по борьбе с организованной преступностью особый акцент сделан на деятельности правоохранительных органов в цифровом пространстве. См.: *Овчинский В., Жданов Ю.* Европа спасается от мафии: о Стратегии ЕС по борьбе с организованной преступностью на 2021–2025 гг. // Завтра. URL: https://zavtra.ru/blogs/evropa_spasaetsya_ot_mafii (дата обращения: 20.08.2021).

2. Противоправные явления в киберпространстве наносят ущерб интересам не только личности, общества, но и государства. Проблемы *обеспечения национальной безопасности в киберпространстве* приобретают особую остроту и с учетом его наднационального характера требуют привлечения к своему решению правоохранительных органов и разведывательных сообществ различных государств. Однако в последнее время отмечается усиление напряженности между государствами в этих вопросах, которое влечет существенное усложнение процедур взаимной правовой помощи.

3. Наблюдается образование особых *криминогенных зон* киберпространства, подлежащих оперативному обслуживанию, к которым могут быть отнесены отдельные сегменты социальных сетей, сайты криминальной направленности и в первую очередь сеть DarkNet («теневой Интернет»)[1]. В DarkNet функционируют свои поисковые и почтовые сервисы, места сетевого общения, торговые площадки, через часть из которых осуществляется торговля наркотиками, оружием, детской порнографией, данными «взломанных» кредитных карт, нелицензионным программным обеспечением. Неотъемлемой частью DarkNet является наиболее популярная в настоящее время анонимная сеть Tor (Onion Router), которая активно используется преступниками. Весь сетевой трафик в ней шифруется и передается сложными маршрутами, что затрудняет определение точного адреса источника и получателя, а законспирированные площадки используются для координации и совершения противозаконных действий. По оценке зарубежных исследователей, до 57% сайтов в сети Tor вовлечены в преступную деятельность (распространение наркотиков, торговля оружием, отмывание денег через криптовалютный рынок, порнография с участием детей и животных)[2].

4. Расширяется накопление в киберпространстве *цифровых следов* преступной деятельности и оперативно значимых данных в компьютерной форме, возникают и места концентрации оперативно-розыскной информации, ранее не контролировавшиеся правоохранительными органами. Объем цифровых следов в боль-

[1] Термином «DarkNet» обозначается сформировавшая в сети Интернет подсистема, которая объединяет технологии и коммуникации, призванные обеспечить анонимность их пользователей (в первую очередь — невозможность определения их реального IP-адреса, сведений об их личности и содержания передаваемых пакетов данных).

[2] См.: *Davies G.* Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers // The Journal of Criminal Law. 2020. Vol. 84. Is. 5. P. 407–426.

шинстве случаев внушителен, что повышает важность их вовлечения в процесс раскрытия и расследования преступлений.

В свою очередь, концентрация существенных объемов оперативно значимой информации в киберпространстве побуждает оперативно-розыскную науку активно изучать специфические формы и методы доступа к ней. Понимание специфики механизмов следообразования в киберпространстве приобретает особое значение для адаптации традиционных криминалистических методик и оперативно-розыскных методов к использованию в новой среде. Поскольку для эффективной работы в DarkNet оперативный сотрудник должен обладать особыми компетенциями, в ряде государств создаются подразделения, специализирующиеся на противодействии киберпреступности[1]. Такие подразделения созданы и в ряде служб центрального аппарата МВД России, и в территориальных органах внутренних дел.

5. Фиксируется нарастание применения «цифровых» *методов противодействия* правоохранительным органам со стороны криминалитета. В обзоре Европола за 2020 г. отмечается, что «в таких областях, как DarkNet, преступники усилили сотрудничество и объединили усилия, чтобы дать ответ на общие проблемы. Это означает, что они могут сделать свой криминальный бизнес более устойчивым и, в частности, использовать более совершенные решения в области безопасности с тем, чтобы правоохранительные органы не могли их отслеживать. В целом киберпреступники демонстрируют повышенный уровень операционной безопасности и доказывают, что хорошо осведомлены о том, как скрыть свою личность и преступную деятельность от правоохранительных органов или компаний частного сектора»[2].

Закрепляясь в киберпространстве, преступность опирается на применение технологий шифрования и криптографических алгоритмов, затрудняющих доступ к скрываемой компьютерной информации и следам криминальной активности. Использование

[1] С 2015 г. в Великобритании функционирует спецподразделение по борьбе с преступностью в DarkNet (Joint Operations Cell, JOC). Подобные подразделения созданы в 2018 г. при Европоле и в 2020 г. при Министерстве юстиции США.

[2] Internet Organised Crime Threat Assessment (IOCTA) 2020 / European Union Agency for Law Enforcement Cooperation, 2020. URL: https://www.europol.europa.eu/iocta-report (дата обращения: 20.08.2021).

криптовалют позволяет существенно усложнить и отслеживание платежей, связанных с преступной деятельностью[1].

6. Особые риски нового порядка влечет повышенный интерес криминала к *технологиям ИИ*[2], в результате применения которых отдельные направления общественно опасной социальной активности могут полностью уйти из поля зрения правоохранительной системы. Использование технологий преступниками нацелено на разработку оптимальных стратегий противоправной деятельности[3], поиск новых «бизнес-моделей» криминальной деятельности, повышающих ее прибыльность и снижающих вероятность выявления правоохранительными органами, совершенствование методов сокрытия следов противоправной активности. Появление на криминальном рынке предложений «*ИИ как услуга*» усиливает доступность этих технологий для субъектов, не обладающих достаточным уровнем технических знаний, но способных профинансировать получение искомого результата.

В аналитическом обзоре, подготовленном в 2020 г. Центром по противодействию киберпреступности Европола[4], утверждается, что уже сегодня основными направлениями использования ИИ криминалом являются:

а) разработка вредоносных программ с усиленными алгоритмами взлома и повышенной скрытностью функционирования;

б) дистанционное управление техническими устройствами «Интернета вещей» (например, элементами «умного дома») для полу-

---

1 Internet Organised Crime Threat Assessment (IOCTA) 2020 / European Union Agency for Law Enforcement Cooperation, 2020. URL: https://www.europol.europa.eu/iocta-report (дата обращения: 20.08.2021).

2 См.: Artificial Intelligence and the Law: Cybercrime and Criminal Liability / ed. D.J. Baker, P.H. Robinson. NY.: Routledge, 2021.

3 По оценкам специалистов, «атаки на основе ИИ могут обходить традиционные системы обнаружения более чем в 15% случаев, в то время как средняя фишинговая атака (без ИИ) может быть успешной только в 0,3% случаев». См.: Защищаемся от ИИ с помощью ИИ: решения с поддержкой искусственного интеллекта для киберугроз нового поколения // Securitylab.ru. URL: https://www.securitylab.ru/analytics/518993.php (дата обращения: 20.08.2021).

4 См.: Europol's European Cybercrime Centre. Malicious Uses and Abuses of Artificial Intelligence. Report, 2020. URL: https://www.europol.europa.eu/publications-documents/malicious-uses-and-abuses-of-artificial-intelligence (дата обращения: 20.08.2021).

чения доступа к конфиденциальным данным и создания условий для совершения противоправных действий[1];

в) манипулирование системами ИИ, управляющими движением транспортных средств и «беспилотников», при подготовке и совершении преступлений;

г) повышение эффективности алгоритмов подбора паролей к зашифрованным данным и взлом систем компьютерной безопасности;

д) усиление устойчивости криптографических систем, используемых для сокрытия следов преступлений;

е) формирование «виртуальной личности» в социальных сетях для совершения мошенничеств;

ж) повышение эффективности методов социальной инженерии с целью выявления потенциальных жертв, сбора конфиденциальной и деловой информации.

В зарубежной литературе называются и иные направления применения технологий ИИ криминалом[2]. Отмечается, что особый интерес к их использованию в свой деятельности проявляют в первую очередь высокоорганизованные преступные сообщества. Приводятся примеры машинного обучения для осуществления мошенничеств в финансовой сфере и манипулирования рынком, при этом системы ИИ разрабатывают оптимальные стратегии, существенно усложняющие обнаружение противоправных действий. Фиксируется использование технологий ИИ при логистическом планировании наркотрафика с использованием роботов и беспилотных транспортных средств[3]. Применение в социальных сетях ботов, автоматически генерирующих потоки сообщений заданной направленности, расширяется не только для продажи наркотиков, но и для распространения дезинформации и компрометирующих материалов в отношении конкурентов[4].

---

1 См.: *Hilt S.*, *Huq N.*, *Rösler M.*, *Urano A.* Cybersecurity Risks in Complex IoT Environments: Threats to Smart Homes, Buildings and Other Structures // Trend Micro. 2019. URL: https://documents.trendmicro.com/assets/white_papers/wp-cybersecurity-risks-in-complex-iot-environments.pdf?_ga=2.20408120.1686390182.1575332885-267397288.1557129106 (дата обращения: 20.08.2021).

2 См.: *King T.C.*, *Aggarwal N.*, *Taddeo M.* Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions // SciEng Ethics. 2019. URL: https://doi.org/10.1007/s11948-018-00081-0 (дата обращения: 20.08.2021).

3 См.: Europol. Serious and organised crime threat assessment. 2017. URL: https://www.europol.europa.eu/socta/2017/ (дата обращения: 20.08.2021).

4 См.: *Mackey T.K.*, *Kalyanam J.*, *Katsuki T.*, *Lanckriet G.* Machine learning to detect prescription opioid abuse promotion and access via Twitter // American Journal of Public Health. 2017. 107 (12). URL: https://doi.org/10.2105/AJPH.2017.303994 (дата обращения: 20.08.2021).

Одним из наиболее ярких примеров виртуализации реальности в условиях цифровизации общества является использование технологий DeepFakes, которые обладают особым криминальным потенциалом[1]. Они позволяют синтезировать изображение заданного человека и подменять лицо в обрабатываемом видеофрагменте, создавая фальсифицированный сюжет, а также применяются для выявления по речевым образцам индивидуальных особенностей речи конкретного человека и синтеза заданных фраз, произносимых его голосом.

Такие технологии уже используют для достижения целого ряда преступных целей. Назовем лишь часть из них.

1. Генерирование чужого изображения для обхода систем биометрической аутентификации в платежных системах и системах доступа.

2. Преследование человека в сети, подрыв его авторитета и нанесение ущерба имиджу в результате размещения сфальсифицированных компрометирующих материалов. Вымогательство с угрозой опубликования фальшивого видеоматериала, который нанесет ущерб репутации физического или юридического лица.

3. Организация кампаний по дезинформации, например, с целью вмешательства в выборы или подстрекательства к насилию, общественным беспорядкам, манипулирования общественным мнением с поддержкой нарративов экстремистских или террористических групп.

4. Мошенничество с ценными бумагами, вмешательство в функционирование финансовых рынков (например, распространение подделки, изображающей исполнительного директора компании, выступающего с заявлением о финансовых потерях или банкротстве).

5. Преступления в интернете в отношении несовершеннолетних с созданием поддельной виртуальной личности, выдающей взрослого человека за подростка.

6. Фальсификация или манипулирование электронными доказательствами. Представление ложного аудиовизуального контента в качестве доказательств с целью воспрепятствовать расследованию уголовных дел. Подобные «подделки» могут стать серьезным вы-

[1] Уже озвучены предложения закрепить в УК РФ их использование при совершении преступлений (мошенничества, вымогательства, оскорбления, клеветы и т.д.) в качестве квалифицирующего признака. См.: *Ларина Е., Овчинский В.* Криминальная жизнь дипфейков: о новой виртуальной реальности, становящейся чрезвычайно опасной // Завтра. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfejkov (дата обращения: 20.08.2021).

зовом современным методам криминалистического анализа и проверки подлинности доказательств, что остро ставит вопрос о необходимости разработки технологий для обнаружения фальсифицированных материалов[1].

Итак, мы показали, как цифровизация общества и виртуализация реальности вызвали нарастание и усложнение особых криминальных явлений, которые могут быть оценены как важные вызовы ОРД. Полагаем, что для нейтрализации неизвестных ранее социальных угроз потребуется не только обеспечить поиск особых организационных и тактических решений, но и произвести *обновление моделей* ОРД и смену ее отдельных теоретических концепций.

Роль ОРД в противодействии преступности в новых условиях возрастает. Как известно, ее разведывательная сущность во многом связана с осуществлением сбора оперативно значимой информации о криминальных явлениях, событиях и лицах, основанного на выполнении активных гласных и негласных действий. Изменение самих принципов функционирования информационного пространства, его расширение за счет применения нового инструментария не могут не отразиться на ОРД. Для нее существенно повышаются требования к выявлению, анализу и оценке достоверности колоссальных объемов цифровых данных, потенциально содержащих оперативно значимую информацию. Напомним, что виртуализирующееся информационное пространство массово заполняется недостоверными и искаженными сведениями, плохо согласующимися между собой, и *поиск смыслов* становится одной из основных задач любой информационной работы. Это справедливо и для ОРД, которая в основном опирается на работу с информацией. Оперативный сотрудник должен не просто обнаружить в информационном потоке необходимые сведения, но и, определив их достоверность и выявив в них смыслы, получить необходимые знания.

Эффективность ОРД в значительной степени определяется также тем, насколько полно учитываются особенности *среды*, в которой она реализуется. Применяемые методы и средства должны быть максимально адаптированы к этим особенностям, чтобы обеспечить скрытный характер проводимых негласно мероприятий. Глу-

[1] Инструменты с поддержкой ИИ, такие как FaceForensics++, уже показали точность обнаружения, превышающую возможности ручного анализа. В сентябре 2020 г. «Microsoft» выпустила новый инструмент для обнаружения подделок Microsoft Video Authenticator, который анализирует содержимое и дает пользователю возможность убедиться в том, что видео могло быть подвергнуто манипуляциям.

бокое понимание оперативным сотрудником природы реализуемых действий и их последствий в специфичной среде является непременным условием обеспечения конспиративности этих действий. С учетом этого с позиций оперативно-розыскной науки важно исследовать влияние цифровизации на специфику следующих сред реализации информационных взаимодействий с целью получения оперативно значимой информации:

- физического пространства — естественной среды реализации таких отношений;
- киберпространства — среды, сформировавшейся на основе взаимодействия пользователей сетей с технологической инфраструктурой и информационными объектами;
- виртуальной реальности — областей киберпространства, имитирующих взаимодействия в обычной реальности;
- дополненной реальности — физического пространства, дополняемого виртуальными информационными объектами за счет применения специальных устройств[1].

Особый интерес представляет киберпространство, в котором уже сложились условия для применения большинства традиционных оперативно-розыскных средств и методов, причем на практике они вполне успешно адаптируются к особенностям этой среды, а их применение сопровождается расширением арсенала средств добывания оперативно значимой информации, информационно-аналитических технологий, специального программного обеспечения и технических средств негласного сбора компьютерной информации.

Оперативные сотрудники при раскрытии преступлений могут применять снятие информации с используемых преступниками технических каналов связи, организовывать исследование изъятых устройств мобильной связи, средств вычислительной техники, носителей компьютерной информации, опираясь на применение мощных программно-аппаратных комплексов. Н.В. Павличенко и А.И. Тамбовцев также указывают на важность использования в ОРД новых *технологий сбора и анализа цифровых следов* социальной активности граждан, образующихся в разнообразных мобильных устройствах фиксации персональной информации. Они убедительно аргументируют это необходимостью компенсировать утрату традиционных информационных источников оперативно

[1] Современный человек значительную часть времени уже проводит в дополненной реальности, получая потоки информации с различных устройств (смартфонов, фитнес-трекеров, планшетов и т.п.).

значимой информации в результате перехода межличностного общения в виртуальное пространство и связанной с этим изоляции людей друг от друга, приводящих к существенному «уменьшению контактов (вплоть до полного их отсутствия), необходимых правоохранительным органам для решения поставленных перед ними задач»[1].

Значительным потенциалом по обнаружению неявных разрозненных сведений, сопоставление которых с применением технологий анализа больших данных дает ценную информацию, обладает сбор данных из открытых (общедоступных) источников, в зарубежной литературе называемый OSINT (*Open Source Intelligence*). Обработка всех доступных сведений с применением современных аналитических технологий дает возможность выявлять латентные преступления, обнаруживать признаки подготовки к совершению преступления, устанавливать неявные связи между изучаемыми лицами, иную оперативно значимую информацию.

Все чаще полиция переходит от пассивного расследования, которое ограничивается сбором информации в открытых общедоступных ресурсах киберпространства, к применению *активных методов*, связанных, в частности, с созданием фальшивых сайтов и виртуальных личностей для создания в сети различного рода «ловушек» для преступников. В киберпространстве могут применяться и особые подходы, основанные на использовании его специфики. Все шире правоохранительными органами практикуется проведение специальных операций в киберпространстве, для которых требуется наличие у оперативного сотрудника особых умений и навыков применения специального программного обеспечения, негласно устанавливаемого в компьютерные устройства подозреваемых[2]. По мнению зарубежных ученых, такие операции проводятся полицией редко «не потому, что такая тактика ограничена законом, а из-за отсутствия опыта, ресурсов и ясности в политике и регламентирующих документах»[3].

---

1 *Павличенко Н.В., Тамбовцев А.И.* Детерминанты современных метаморфоз оперативно-розыскных мероприятий // Труды Академии управления МВД России. 2020. № 3 (55). С. 38–50.

2 См.: *Осипенко А.Л.* Сбор информации и полицейские операции по противодействию организованной преступности в киберпространстве: зарубежный опыт // Общество и право. 2021. № 1. С. 47–55.

3 *Davies G.* Shining a Light on Policing of the Dark Web: An Analysis of UK Investigatory Powers // The Journal of Criminal Law. 2020. Vol. 84. Is. 5. P. 407–426.

В то же время с учетом широкого применения преступниками технологий шифрования и анонимизации в киберпространстве необходимую информацию без применения подобных мер добыть чаще всего невозможно. Поскольку применение специализированного программного обеспечения для дистанционного доступа к целевым устройствам подозреваемых предполагает существенное ограничение прав граждан и способно привести к нарушениям норм международного права при трансграничных действиях в отношении компьютеров, расположенных на территории других государств, оперативно-розыскная наука призвана обеспечить поиск приемлемых решений в области правовой регламентации, организации и тактики проведения мероприятий, связанных с дистанционным внедрением специального программного обеспечения, предусмотрев гарантии защиты прав третьих лиц и меры, исключающие нанесение ущерба нецелевым сетевым устройствам.

В решении своих задач ОРД всегда опиралась на достижения научно-технической сферы, проявляя интерес к применению специальных технических средств и новых технологических решений, обеспечивающих возможность негласного сбора оперативно значимой информации. Особое место в новых концепциях реализации ОРД должны занять технологии ИИ, аналитика больших данных, которые также могут рассматриваться как особый элемент виртуальной реальности. Внедрение этих технологий позволяет кардинально изменять подходы к функционированию оперативно-розыскных учетов, пересматривать принципы работы с оперативно значимой информацией. Переход к использованию особых аналитических технологий и технологий ИИ дает возможность обрабатывать массивы неструктурированной информации и на этой основе эффективно решать сложные *задачи*, такие как:

— идентификация по различным признакам подозреваемых и разыскиваемых лиц (голос, лицо, походка и др.); обнаружение в скоплении людей лиц, находящихся в розыске либо социально опасных, с отклонениями в поведении;

— определение маршрутов перемещений (с учетом данных геолокации и записей камер наблюдения), продолжительности пребывания на объектах, контактов с конкретными лицами;

— выявление устойчивых связей, основных способов коммуникации, обобщение данных о состоявшихся сеансах связи (продолжительности и периодичности), финансовых транзакциях, покупках;

— фиксация особенностей физического состояния разрабатываемых лиц, их физической и сетевой активности, интересов и спо-

собов проведения досуга, психологического и эмоционального состояния при сетевом общении;

— автоматизированное выявление оперативно значимых сведений и признаков, свидетельствующих о скрываемой криминальной активности; формирование уведомлений об изменениях в профилях изучаемых лиц, указывающих на потенциальную преступную деятельность;

— определение состава преступных групп, распределения обязанностей между их участниками; прогнозирование их криминальной активности.

Это далеко не полный перечень решаемых задач. Для его расширения оперативно-розыскная наука должна на постоянной основе выявлять и обобщать все возможности, открывающиеся за счет внедрения новых информационно-аналитических технологий, вырабатывать методические рекомендации по их использованию оперативными сотрудниками.

В то же время с позиций ОРД технологии искусственного интеллекта в их сегодняшнем состоянии имеют важные *ограничения*, с учетом которых применять их необходимо с осторожностью, особенно там, где от их результатов зависит ограничение прав граждан. В значительной степени результативность их применения определяется полнотой и достоверностью исходных данных и качеством закладываемых разработчиками правил их обработки. Причем технологии ИИ в основном рассчитаны на решение задач с фиксированными правилами, а в сфере ОРД эти правила могут резко меняться. На оценке предлагаемых решений сказывается и непрозрачность алгоритмов, применяемых в ИИ, их потенциальная подверженность случайным либо преднамеренным ошибкам. Кроме того, как уже отмечалось, при решении задач ОРД важно не только выявлять факты и связи, но и постигать их смысл, что пока реализуемо только при участии опытного аналитика. Таким образом, ИИ в настоящее время продуктивен только при решении типовых задач с фиксированным набором проверенных правил и массивом достоверных исходных данных и недостаточно эффективен в ситуациях, требующих творческого подхода.

Следует отметить, что определенная потенциальная опасность ИИ привела к появлению в ЕС законопроекта, предусматривающего детальную регламентацию его применения. Предусмотрено запрещение использования систем ИИ с неприемлемо высоким риском, к которым отнесены следующие системы: «манипулирующие человеческим поведением, влияющие на свободу выбора человека; поощряющие опасное поведение несовершеннолетних;

позволяющие осуществлять социальный скоринг (моделирование поведения человека или его классификацию при помощи ИИ-анализа его поведения в соцсетях)». Системами ИИ с высоким риском предложено считать: «все системы с удаленной биометрической идентификацией; автоматическую оценку кредитоспособности гражданина; используемые правоохранительными органами системы ИИ, которые могут ущемлять права человека». Их применение предполагает получение разрешения суда и должно быть ограничено узкими задачами — например, «поиском пропавших детей, предотвращением террористической угрозы, поиском и идентификацией находящегося в розыске преступника или террориста» и т.п.[1]

Тем не менее высокий прогностический потенциал технологий ИИ и эффективность их при выборе оптимальных управленческих решений обеспечивают надежную основу для перехода на *упреждающую модель* организации полицейской деятельности, предполагающую учет и анализ оперативной информации во всей полноте и применение предиктивной аналитики[2]. Последняя обеспечит оперативное выявление признаков, указывающих на проявления противоправной активности, требующей реакции со стороны правоохранительных органов. Отметим, что для реализации указанной модели особую важность имеет законодательно закрепленное обеспечение доступа оперативных подразделений к массивам оперативно значимых данных (больших данных) и в первую очередь наличия правовой основы такого доступа.

Важное место во внедрении упреждающей модели должно занять совершенствование форм и методов оперативно-розыскного контроля, обеспечивающего мониторинг поведения отдельных категорий граждан для пресечения криминальных действий с их стороны. По справедливому замечанию В.С. Овчинского, «успешная реализация подобного подхода предполагает коренное и полное изменение функционала, организационной структуры и отчетности полицейских органов»[3].

---

[1] Европа поставит распознавание лиц на место // Коммерсантъ. 2021. 21 апр. URL: https://www.kommersant.ru/doc/4782746 (дата обращения: 20.08.2021).

[2] В. Колокольцев выступил на пленарном заседании Международного полицейского саммита // Официальный сайт МВД России. URL: https://мвд.рф/news/item/18681665/ (дата обращения: 20.08.2021).

[3] *Овчинский В.* Полиция 4.0: как реорганизовать полицию в условиях технологической революции // Завтра. URL: http://zavtra.ru/blogs/politciya_4_0_ (дата обращения: 20.08.2021).

Способствовать этому должны также наращивание систем видеонаблюдения с использованием ИИ и масштабный мониторинг информационных ресурсов сети Интернет, а также комплекс иных мер обеспечительного характера (организационных, технических, правовых). Основные технологии цифрового контроля уже активно применяются в полицейской деятельности многих государств. Это и фиксация передвижений и контактов граждан по данным операторов мобильной связи, и сбор персональных данных и информации о финансовых транзакциях, и применение видеокамер с системой распознавания лиц.

В нашей стране уже реализуются социальные проекты, представляющие несомненный интерес с точки зрения достижения целей ОРД. В основу цифровой стратегии Москвы «Умный город — 2030», разработанной Департаментом информационных технологий г. Москвы в 2018 г., заложено применение технологий искусственного интеллекта для анализа данных из различных источников и подготовки решений для правительства. Главными поставщиками информации о местонахождении и маршрутах перемещений граждан стали операторы сотовой связи. В апреле 2020 г. принят Федеральный закон «О проведении эксперимента по установлению специального регулирования в целях создания необходимых условий для разработки и внедрения технологий искусственного интеллекта в субъекте Российской Федерации — городе федерального значения Москве». Реализация госпрограммы Москвы «Безопасный город» в 2020 г. способствовала раскрытию более 5 тыс. преступлений, а использование системы распознавания лиц позволило к марту 2021 г. выявить и задержать в Москве свыше 260 граждан, находящихся в федеральном розыске[1].

Отдельно следует обсудить обусловленную развитием информационно-коммуникационных технологий необходимость обновления системы ОРМ, закрепленной Федеральным законом от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности». Она уже давно требует пересмотра в первую очередь с точки зрения уточнения перечня специальных технических мероприятий и определения места в ней информационно-аналитических мероприятий.

Обратим внимание на то, что в законодательстве многих государств уже регламентированы действия по доступу к информации

[1] См.: Искусственный интеллект на службе полиции // Вестник ГЛОНАСС. URL: http://vestnik-glonass.ru/news/intro/iskusstvennyy-intellekt-na-sluzhbe-politsii/ (дата обращения: 20.08.2021).

в киберпространстве. Так, в США негласный дистанционный доступ к компьютеру подозреваемого определен как «метод сетевого расследования» (*network investigative techniques — NIT*) и закреплен с 2016 г. поправкой к Правилу 41 Федеральных правил уголовного судопроизводства. Ордер на производство этого действия разрешает установку специального программного обеспечения на компьютер (смартфон, планшет и т.п.) без уведомления его владельца, наблюдение за подозреваемым и сбор информации о нем, копирование хранимой на устройстве информации и дистанционное включение встроенных микрофонов и видеокамер[1]. В Великобритании те же действия закреплены с 2016 г. в Законе о полномочиях при расследовании (Investigatory Powers Act 2016). Они предполагают как физическое (копирование данных с устройства, к которому получен физический доступ), так и дистанционное (установка программного обеспечения через сеть) вмешательство в функционирование оборудования с целью получения: данных об оборудовании; данных о сеансах связи и передаваемых сообщениях; другой информации[2].

Мы уже предлагали объединить действия, предусмотренные ОРМ «получение компьютерной информации», «прослушивание телефонных переговоров» и «снятие информации с технических каналов связи» (а также частично «контроль почтовых отправлений, телеграфных и иных сообщений»), в едином мероприятии, присвоив ему название «получение информации из технических устройств, систем и каналов связи»[3]. Это позволило бы снять на практике многие противоречия, возникающие при осуществлении названных ОРМ, разрешило бы неоднозначность, возникающую в случае доступа субъектов ОРД к сообщениям электронной почты, данным чатов, мессенджеров, онлайн-телефонии.

Что же касается закрепления в законе оперативно-розыскных методов «аналитический поиск», «оперативное распознание», «оперативно-розыскное прогнозирование», важность которого отмеча-

---

1 См.: *Granick J.S.* Challenging Government Hacking Whats Stake // ACLU. 2017. URL: https://www.aclu.org/blog/privacy-technology/internet-privacy/challenging-government-hacking-whats-stake (дата обращения: 20.08.2021).

2 См.: Investigatory Powers Act 2016 // Legislation.gov.uk. URL: https://www.legislation.gov.uk/ukpga/2016/25/contents/enacted (дата обращения: 20.08.2021).

3 См.: *Осипенко А.Л.* Оперативно-розыскная деятельность в информационном обществе: адаптация к условиям цифровой реальности // Научный вестник Омской академии МВД России. 2019. № 4. С. 38–46.

ется учеными[1], это, на наш взгляд, следует сделать, объединив их в одной группе, которую можно было бы обозначить как «автоматизированный информационно-аналитический поиск». В то же время соответствующие действия отличаются от ОРМ, предполагающих получение оперативно значимых сведений из конкретных объектов (от конкретных субъектов). Они направлены на добывание «новых знаний о разведываемом объекте или явлении на основании аналитической обработки добытой информации и сведений об известных фактах»[2]. С учетом этого логично было бы относить данные действия не к ОРМ, а к мерам обеспечения оперативно-розыскного производства, которые могли бы определяться в законе особо[3].

Поводя итоги, обобщим основные вопросы, изучению которых в условиях цифровизации важно уделить повышенное внимание с позиций оперативно-розыскной науки. К ним, на наш взгляд, относятся:

- специфика криминальных процессов и угроз, обусловленных информатизацией общества и виртуализацией реальности, их влияние на изменение характера оперативно-розыскной деятельности;
- влияние на организацию и тактику ОРД трансформаций современной преступности и использования новых информационных технологий в криминальной деятельности;
- специфика киберпространства, в первую очередь его «теневых» сегментов и криминогенных объектов, особенности организации их оперативного обслуживания;
- особенности сетевых организованных преступных формирований и их взаимодействия, усложнение принципов управления ими и координации их деятельности, специфика оперативного внедрения в них и контроля за связанными с ними сетевыми ресурсами;
- закономерности концентрации оперативно значимой информации в киберпространстве, определение способов доступа к ней при осуществлении оперативно-розыскных мероприятий;
- оптимальные варианты адаптации традиционных средств и методов ОРД к применению в новой информационной среде

---

1 См.: *Денисов В.В., Яковец Е.Н.* Сущность и содержание информационно-аналитического обеспечения полицейской разведки // Труды Академии управления МВД России. 2017. № 1 (41).

2 *Овчинский С.С.* Оперативно-розыскная информация. М., 2000.

3 См.: *Луговик В.Ф., Осипенко А.Л.* Оперативно-розыскная деятельность органов внутренних дел: перспективы совершенствования правового регулирования // Вестник Воронежского института МВД России. 2015. № 4.

и в дополненной реальности, возможности использования в решении задач ОРД средств виртуальной и дополненной реальности, специальных технических средств для сбора компьютерной информации;

- укрепление взаимодействия субъектов ОРД с иными участниками противодействия организованной преступности в киберпространстве, в том числе с зарубежными, оптимизация доступа к информационным ресурсам и организации обмена оперативной информацией;
- направления применения аналитических технологий с учетом возможностей ИИ, выявление среди них наиболее перспективных и адаптация их к решению задач оперативно-розыскной деятельности, внедрение методов предиктивной аналитики, формирование с использованием технологий ИИ модифицированной системы оперативно-розыскного контроля;
- специфика доступа к информации, зашифрованной с целью сокрытия признаков и следов криминальной деятельности;
- особенности осуществления негласных действий в киберпространстве, создания и использования с этой целью виртуальных личностей и контролируемых оперативными сотрудниками сетевых объектов;
- требования к оперативно-розыскным методам получения цифровых данных для вовлечения их в уголовный процесс;
- подходы к обеспечению собственной информационной безопасности оперативных подразделений, осуществляющих ОРМ в киберпространстве.

Очевидно, этот перечень может и должен расширяться по мере развития технологий и общественных отношений, связанных с цифровизацией общества.

Добавим, что эффективное решение задач ОРД в киберпространстве невозможно без технического перевооружения оперативных подразделений. Необходима организация работы мощных дата-центров и центров обработки данных, способных обеспечить хранение и обработку больших объемов данных, а также информационно-телекоммуникационной инфраструктуры, обеспечивающей безопасную и устойчивую высокоскоростную передачу данных между дата-центрами и оконечными устройствами. Долговременное хранение массивов оперативно значимой информации позволит использовать ее не только как ориентир для принятия оперативных решений, но и как ценный ресурс, обеспечивающий эффективность ОРД в целом. При внедрении программного обеспечения важно опираться на продуманную стратегию, предусмат-

ривающую общую инвентаризацию уже используемых разноформатных программ и баз данных, установление их совместимости, интеграцию их в единую систему, выявление и адаптацию к решению задач ОРД перспективных программных комплексов, представленных в общем обороте, и подготовку заданий на разработку особых специализированных комплексов, соблюдение общих требований по совместимости для всех внедряемых комплексов.

Нельзя не упомянуть важность существенного обновления системы подготовки, переподготовки и повышения квалификации кадров с учетом нового набора компетенций, которыми должен обладать оперативный сотрудник для эффективного осуществления ОРД в изменившихся условиях.

Отметим и особую важность решения проблем, связанных с контролем за самой ОРД. По оценке В.С. Овчинского, «в условиях цифровизации полиция использует все более сложные технологии, которые могут нести потенциальную угрозу информационной безопасности граждан и нормам общественной морали. Для того чтобы предупредить формирование негативных тенденций, общество должно следить, является ли деятельность полиции максимально открытой и подконтрольной. Этические проблемы, связанные с работой полиции, могут быть решены с помощью совершенствования технологий и соответствующего регулирования и общественного контроля»[1].

Наконец, подчеркнем, что нарастание остроты противостояния с криминалом в киберпространстве должно получить соответствующий отклик в науке и практике ОРД, связанный с усилением решительности в поиске и выборе новых средств и методов, поскольку в этой сфере потеря тактической и стратегической инициативы привела бы к утрате принципиальных позиций правоохранительной системы, вернуть которые будет гораздо сложнее, чем удержать.

---

[1] Этика и «цифра»: этические проблемы цифровых технологий. М.: РАНХиГС, 2020.

Е.Н. Яковец

К вопросу о сущности и содержании оперативно-розыскного мероприятия «получение компьютерной информации»

Получение компьютерной информации (ПКИ) занимает особое место среди ОРМ. В современном мире виртуальные данные сопровождают человека буквально на каждом шагу. Они концентрируются в информационных системах, циркулируют в сети Интернет, других информационно-телекоммуникационных сетях. В связи с этим в оперативно-розыскной науке и практике ведется активный поиск оптимальных форм и методов сбора компьютерной информации, представляющей оперативный интерес. При этом, как правило, отмечается недостаточная правовая регламентация получения доступа к компьютерным данным в интересах ОРД. До недавнего времени вариант законодательного закрепления соответствующих действий был предложен лишь в модельном законе «Об оперативно-розыскной деятельности (новая редакция)», принятом на XXVII пленарном заседании Межпарламентской Ассамблеи государств — участников СНГ (постановление от 16 ноября 2006 г. № 27-6), где данное мероприятие именуется «*мониторинг информационно-телекоммуникационных сетей и систем*» и определяется как «*получение сведений, необходимых для решения конкретных задач ОРД, и их фиксация путем наблюдения с применением специальных технических средств за характеристиками электромагнитных и других физических полей, возникающих при обработке информации в информационных системах и базах данных и ее передаче по сетям электрической связи, компьютерным сетям и иным телекоммуникационным системам*». В принципе данное определение верно по своей сути и его можно принять за основу для дальнейших рассуждений.

Основные криминалистические особенности компьютерной информации заключаются в следующем:

1) она достаточно просто и быстро *преобразуется* из одной объектной формы в другую, *копируется* (размножается) на различные виды машинных носителей и *пересылается на любые расстояния*, ограниченные только радиусом действия современных средств электросвязи;

2) при изъятии компьютерной информации, в отличие от изъятия материального предмета (вещи), она *сохраняется в первоисточнике*;

3) в случае необходимости доступ к ней могут иметь одновременно *несколько пользователей сети ЭВМ*.

Выделяется *два основных вида* компьютерной информации — *общего пользования* (общедоступная) и *охраняемая законом* (ограниченного доступа).

К сведениям ограниченного доступа относится та компьютерная информация, которая удовлетворяет двум обязательным условиям:

— она должна быть документированной — зафиксированной на материальном носителе, с реквизитами, позволяющими ее идентифицировать;

— доступ к такой информации должен ограничиваться в соответствии с законодательством Российской Федерации[1].

Компьютерная информация обладает также особым свойством, которое активно используется злоумышленниками при совершении противоправных деяний. Это обезличенный характер последней (отсутствие признаков, прямо указывающих на связь с подозреваемым), а также возможность ее быстрого и полного уничтожения.

Понятие компьютерной информации на уровне отечественного законодательства закреплено лишь в гл. 28 УК РФ, где в примечании 1 к ст. 272 («Неправомерный доступ к компьютерной информации») отмечено, что под этим термином следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Таким образом, под компьютерной информацией подразумевается не какой-то особый вид информации, а лишь специфическая *форма* ее представления, приспособленная для обработки с помощью средств компьютерной техники.

Средства компьютерной техники, как известно, по своему функциональному назначению подразделяются на две основные группы: 1) аппаратные средства (Hard Ware); 2) программные средства (Soft Ware).

Под *аппаратными средствами* понимаются механические, электрические и электронные технические устройства, используемые для систематизации и обработки данных. К ним относятся:

[1] *Вехов В.Б.* Криминалистическая характеристика преступлений в сфере компьютерной информации // Киберпол.ру. URL: http://www.cyberpol.ru/public/metodica_vehov-p1.doc (дата обращения: 09.06.2020).

1) персональный компьютер (ПК) — комплекс технических средств, предназначенных для автоматической обработки информации в процессе решения вычислительных и информационных задач (персональные и сетевые компьютеры, серверы, ноутбуки, сотовые телефоны, смартфоны, планшеты, банкоматы и др.). ПК является *оконечным оборудованием обработки данных*, которое предназначено для преобразования пользовательской информации в данные для передачи по линиям связи (кодирование) и осуществления обратного преобразования (декодирование). Таким образом, ПК может являться средством передачи информации, ее получателем или тем и другим одновременно. Компьютерная информация может на некоторое время «задерживаться» в микросхемах памяти ПК.

Передача и (или) прием компьютерной информации посредством использования ПК предполагает наличие линий связи и каналов связи[1]. В качестве таковых рассматриваются информационно-телекоммуникационные сети (ИТКС). При обработке на промежуточных сетевых устройствах (серверах, маршрутизаторах, концентраторах, модемах и др.) компьютерная информация может оставлять *цифровые следы*;

2) периферийное оборудование — аппаратные средства, имеющие в информационной системе подчиненный кибернетический статус (принтеры, сканеры, факсы и др.). В их микросхемах также может временно накапливаться компьютерная информация;

3) физические носители компьютерной информации, перечень которых достаточно широк (встроенные и внешние накопители на жестких магнитных дисках, флеш-карты, CD-диски, DVD-диски и др.). На этих носителях такая информация сохраняется длительное время и переносится с одного ПК на другой.

Под *программными средствами* компьютерной техники в соответствии с положениями ст. 1261 ГК РФ понимается представляемая в объективной форме совокупность данных и команд, предназначенная для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, получаемые в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

---

[1] См.: Основы телекоммуникаций // URL: http://www.vicgain.ru/modems/1.htm (дата обращения: 01.03.2021).

Практически все ОРМ, фигурирующие в ч. 1 ст. 6 ФЗ об ОРД[1], нацелены на получение оперативно-розыскной информации в той или иной форме (в устной или текстовой, в форме видео- или аудиозаписи, фотоизображения и т.д.). Некоторые из них допускают получение результатов ОРМ и в виде компьютерных файлов (снятие информации с технических каналов связи, наведение справок, сбор образцов для сравнительного исследования, обследование помещений, зданий, сооружений, участков местности и транспортных средств и др.). В связи с этим ПКИ как оперативно-розыскное мероприятие отражает *способ* получения оперативно-розыскной информации, представленной в компьютерной (виртуальной) форме.

Следует подчеркнуть, что до издания Федерального закона от 6 июля 2016 г. № 374-ФЗ (так называемый Закон Яровой)[2] ПКИ охватывалось содержанием таких ОРМ, как «снятие информации с технических каналов связи» и «контроль почтовых отправлений, телеграфных и иных сообщений» (в последнем случае — в качестве средства слежения за электронной почтовой перепиской), с которыми оно имеет много общего. Вполне очевидно, что решение о закреплении ПКИ в качестве самостоятельного ОРМ связано с *широчайшей распространенностью* компьютерной формы представления оперативно значимой информации и специфическими свойствами последней, обусловливающими особые способы ее получения, а также *исключительной важностью* в плане противодействия киберпреступности.

Что же представляют собой преступления, совершаемые в виртуальной среде, с информационной и уголовно-правовой точек зрения?

Как отмечают некоторые авторы, единого понимания рассматриваемого вида преступлений современной наукой и практикой пока еще не выработано. В отечественных и зарубежных изданиях преступления, совершаемые в компьютерных и телекоммуникационных системах, интерпретируются по-разному: «компьютерные преступления», «преступления в сфере высоких технологий», «информационные преступления», «киберпреступления», «преступления в сфере безопасности обращения компьютерной ин-

[1] Об оперативно-розыскной деятельности: Федеральный закон от 12 августа 1995 г. № 144-ФЗ // Российская газета. 1995. 18 авг. Далее — ФЗ об ОРД.

[2] О внесении изменений в Федеральный закон «О противодействии терроризму» и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности: Федеральный закон от 6 июля 2016 г. № 374-ФЗ. Ст. 3 // Российская газета. 2016. 8 июля.

формации», «преступления в сфере компьютерной информации» и др. Такое терминологическое разнообразие понятий связано с отсутствием единого понимания специфики рассматриваемых преступлений, небольшим числом научных изысканий во всех сферах науки, направленных на изучение киберпреступлений[1].

Профессор А.Л. Осипенко использует для обозначения совокупности рассматриваемых преступных деяний понятие *преступлений в глобальных компьютерных сетях* (*сетевых компьютерных преступлений*), которые ввиду многопланового механизма совершения требуют, по его мнению, поиска новых криминалистических и оперативно-розыскных подходов к их выявлению, раскрытию и расследованию[2], а известный американский специалист по проблемам киберпространства Д.Л. Шиндер[3] за весьма пространные и «размытые» дефиниции, связанные с содержанием компьютерных преступных деяний, подвергает резкой критике даже Европейскую конвенцию о киберпреступности[4].

Э. Мелик отмечает в этой связи, что машинная информация одновременно рассматривается и в качестве объекта, и в качестве орудия преступления. Наряду с ней в разряд орудий совершения подобных преступлений попадают сам компьютер, а также информационно-телекоммуникационная сеть (вычислительная среда, в которой эта информация циркулирует). С учетом сказанного, по ее мнению, можно выделить следующие характерные особенности компьютерного преступления: 1) неоднородность предмета посягательства; 2) особенности машинной информации, рассматриваемой как в качестве предмета, так и в качестве средства (орудия) совершения преступления; 3) многообразие предметов и средств преступного посягательства; 4) особенности компьютера и компьютерной сети в целом, рассматриваемых и в качестве предметов, и в качестве средств совершения преступления. Поэтому в качестве

---

1 *Шевченко Е.С.* Тактика производства следственных действий при расследовании киберпреступлений: автореф. дис. ... канд. юрид. наук. М.: МГЮА, 2016. С. 14.

2 *Осипенко А.Л.* Сетевая компьютерная преступность: теория и практика борьбы: монография. Омск: Омская академия МВД России, 2009. С. 109–110.

3 Scene of the Cybercrime: Computer Forensics Handbook / D. Littlejohn Shinder, E. Tittel (eds.); пер. с англ. Т. Тропиной. Владивосток: ВЦИОП при Юридическом институте ДВГУ, 2003. С. 4.

4 Конвенция о преступности в сфере компьютерной информации (ETS № 185). Заключена в г. Будапеште 23 ноября 2001 г. // Сейчас.ру. URL: http://www.lawmix.ru/abro.php?id=3454 (дата обращения: 24.01.2021).

основного классифицирующего признака принадлежности преступления к разряду компьютерных следует выделить словосочетание «*использование средств компьютерной техники*», независимо от того, на какой стадии преступления она использовалась: при его подготовке, в ходе совершения или для сокрытия[1].

Автор данной статьи, соглашаясь с высказанными точками зрения, полагает, тем не менее, что киберпреступления являются одной из разновидностей так называемых *информационных преступлений*, в связи с чем *под компьютерными преступлениями* (*киберпреступлениями*) *следует понимать предусмотренные уголовным законом общественно опасные деяния*, *посягающие на информационную безопасность личности*, *общества и государства*, *совершаемые с использованием средств электронно-вычислительной* (*компьютерной*) *техники*.

Как показывает практика, в своей профессиональной деятельности оперативные подразделения органов, уполномоченных на осуществление ОРД, в зависимости от своей компетенции могут сталкиваться со следующими видами киберпреступлений:

— сбыт наркотических средств, психотропных веществ или их аналогов, совершаемый с использованием информационно-телекоммуникационных сетей, включая сеть Интернет, квалифицируемый по признакам п. «б» ч. 2 ст. 228.1 УК РФ («Незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ или их аналогов, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества»);

— мошенничество в сфере компьютерной информации (ст. 159^6 УК РФ);

— распространение или оборот с помощью сети Интернет порнографических материалов, подпадающее под признаки п. «б» ч. 3 ст. 242 УК РФ («Незаконные изготовление и оборот порнографических материалов или предметов»), п. «г» ч. 2 ст. 242.1 УК РФ («Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних»), а также п. «г» ч. 2 ст. 242.2 УК РФ («Использование несовершеннолетнего в целях изготовления порнографических материалов или предметов»);

— распространение через интернет материалов экстремистского характера, подпадающее под признаки ст. 282.1 УК РФ («Ор-

[1] *Мелик Э.* Компьютерные преступления // Eleonora Melik. URL: http://www.melik.narod.ru/ (дата обращения: 09.01.2021).

ганизация экстремистского сообщества») и ст. 282.2 УК РФ («Организация деятельности экстремистской организации»), которые тесным образом связаны с терроризмом.

Известны и другие виды киберпреступлений, представляющих высокую общественную опасность, включая организацию через интернет заказных убийств[1] и склонение к самоубийству, а также различные виды вымогательства[2].

Выступая на расширенном заседании коллегии МВД России 3 марта 2021 г., Президент Российской Федерации В.В. Путин отметил, что количество преступлений в сфере информационных технологий за последние шесть лет возросло более чем в 10 раз. «Понятно, сами технологии быстро развиваются, мы за ними, к сожалению, не успеваем, — подчеркнул он. — Все мы хорошо понимаем при этом, что за развитием электронной торговли, за предоставлением в глобальной сети разного рода услуг, включая финансовые услуги, — за этим, конечно, будущее. Технологии здесь обновляются и меняются стремительно, но и поле для преступлений, для разного рода аферистов, к сожалению, тоже увеличивается.

Ваша задача — эффективно ответить на этот криминальный вызов, защитить граждан и добросовестный бизнес, который активно осваивает цифровое пространство. Для этого важно своевременно информировать людей о способах защиты от мошенников, повышать профессиональную подготовку и техническое оснащение органов внутренних дел. И конечно, нужно наладить более четкое взаимодействие с банковским сообществом, интернет-провайдерами, операторами сотовой связи.

В целом показатели раскрываемости кибер- и других видов преступлений должны год от года расти. Обращаю внимание — конечно, не за счет статистики, не за счет бумажной отчетности, а благодаря кропотливой работе “на земле”. От этого зависит реализация важнейшего правового принципа — неотвратимости наказания, а значит, и вера людей в справедливость, в силу закона, в способность государства защитить безопасность человека...

---

[1] *Ищенко Е.П.* Новые информационные технологии обеспечения раскрытия и расследования преступлений // Международный круглый стол «Проблемы использования специальных знаний в уголовном производстве». URL: http://kkrimlguvd.org.ua/conferences/article/3 (дата обращения: 07.02.2021).

[2] *Степанова Ю.* Мошенники научились ботать. Информацию из Telegram начали использовать для шантажа // Коммерсант. 2021. 2 марта. URL: https://www.kommersant.ru/doc/4711513 (дата обращения: 02.03.2021).

Мы с вами, к сожалению, знаем, что такое интернет и как он используется для продвижения совершенно неприемлемого контента: для распространения детской порнографии, проституции, для доведения несовершеннолетних до самоубийств, — отметил далее В.В. Путин. — Но кто бы и под каким бы то ни было предлогом, под каким бы то ни было соусом ни пытался хладнокровно использовать детей для достижения своих собственных эгоистических "хорьковых" целей, мы никогда не должны забывать о том, что это наши дети, и работать нужно так, чтобы не создавать дополнительных угроз для их жизни и здоровья»[1].

После данного небольшого отступления вновь обратимся к сущности и содержанию ПКИ.

Нормативная регламентация рассматриваемого ОРМ определена п. 15 ч. 1 ст. 6 ФЗ об ОРД. Отдельные моменты, связанные с его осуществлением, нашли отражение и в других нормах ФЗ об ОРД: ч. 4 ст. 6 и ч. 2 ст. 8, а также в ст. 53, 63, 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи»[2], ч. 5 ст. 15 Федерального закона от 3 апреля 1995 г. № 40-ФЗ «О федеральной службе безопасности»[3], пп. 3.1, 4, 6 ст. 10.1; пп. 2 п. 2, п. 3 ст. 15.8 Федерального закона от 27 июля 2006 г № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[4].

Кроме того, к регламентации ПКИ имеют отношение следующие нормативные правовые акты:

— уже упоминавшаяся выше *Конвенция о преступности в сфере компьютерной информации* (*ETS № 185*). Заключена в г. Будапеште 23 ноября 2001 г. (Российская Федерация к данной Конвенции не присоединилась[5]);

---

1 Выступление Президента Российской Федерации В.В. Путина на расширенном заседании коллегии МВД России 3 марта 2021 г. // Официальный сайт Президента России. URL: http://www.kremlin.ru/catalog/persons/310/events/65090 (дата обращения: 04.03.2021).

2 Российская газета. 2003. 10 июля.

3 Российская газета. 1995. 12 апр.

4 Российская газета. 2006. 29 июля.

5 Нашей стране не удалось договориться о приемлемых для себя условиях трансграничного доступа к компьютерным системам. В марте 2008 г. по инициативе Президента РФ было признано утратившим силу ранее принятое распоряжение от 15 ноября 2005 г. № 557-рп «*О подписании Конвенции о киберпреступности*», в соответствии с которым Россия оставляла за собой право определиться с участием в Конвенции при условии пересмотра положений п. «b» ст. 32. Тем не менее большинство положений данной Конвенции являются ориентиром для российских государственных органов в ходе международного сотрудничества в данной области.

— *Доктрина информационной безопасности Российской Федерации*, утвержденная Указом Президента РФ от 5 декабря 2016 г. № 646[1];

— *Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы*, утвержденная Указом Президента РФ от 9 мая 2017 г. № 203[2];

— *Перечень видов специальных технических средств, предназначенных* (*разработанных*, *приспособленных*, *запрограммированных*) *для негласного получения информации*, утвержденный постановлением Правительства РФ от 1 июля 1996 г. № 770[3];

— *Правила взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность*, утвержденные постановлением Правительства РФ от 27 августа 2005 г. № 538[4];

— *Правила хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приема, передачи, доставки и* (*или*) *обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации*, утвержденные постановлением Правительства РФ от 31 июля 2014 г. № 759[5], и др.

Для реализации результатов ПКИ в уголовном процессе применяется *Инструкция о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд*, утвержденная приказом МВД России, МО России, ФСБ России, ФСО России, ФТС России, СВР России, ФСИН России, ФСКН России, СК РФ от 27 сентября 2013 г. № 776/703/509/507/1820/42/535/398/68[6].

ПКИ наряду со *снятием информации с технических каналов связи* (СИТКС) и *прослушиванием телефонных переговоров* (ПТП) относится к классу оперативно-технических мероприятий (ОТМ). Как известно, для их технического обеспечения на сетях доку-

---

1 Собрание законодательства РФ. 2016. № 50. Ст. 7074.

2 Официальный сайт Президента России. URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 24.02.2021).

3 Собрание законодательства РФ. 1996. № 28. Ст. 3382.

4 Российская газета. 2005. 2 сент.

5 Российская газета. 2014. 6 авг.

6 Российская газета. 2013. 13 дек.

ментальной электросвязи, используемых с целью предоставления услуг передачи данных телематических служб[1], создана Система технических средств по обеспечению оперативно-розыскных мероприятий (СОРМ). Ее технические требования регламентированы приказом Государственного комитета РФ по связи и информации от 27 марта 1999 г. № 47. *Порядок внедрения Системы технических средств по обеспечению оперативно-розыскных мероприятий на сетях телефонной, подвижной и беспроводной связи и персонального радиовызова общего пользования* утвержден приказом Минсвязи России от 25 июля 2000 г. № 130[2].

Действия оперативников, осуществляющих ПКИ, нацелены на проникновение в аппаратные компьютерные средства (ПК, периферийные устройства, ИТКС, носители информации), принадлежащие подозреваемым в совершении преступлений лицам, с помощью определенных способов, которые предполагают использование специальных технических или программных средств, с целью копирования компьютерной информации, представляющей оперативный интерес.

К таким способам, в частности, могут быть отнесены:

- негласное применение специального программного обеспечения и оборудования для скрытного съема данных на закрытых сетевых ресурсах, которые могут представлять потенциальный оперативный интерес;
- оперативно-розыскной мониторинг сетевых информационных ресурсов, представляющих оперативный интерес, который реализуется через автоматизированный поиск ресурсов, содержащих запрещенную к распространению информацию; изучение материалов, связанных с деятельностью организованных преступных сообществ; контроль закрытых для общего доступа мест сетевого общения представителей криминальной среды;
- негласная установка в компьютерные устройства, принадлежащие разрабатываемым лицам, специального программного обеспечения, позволяющего фиксировать содержание осуществляемых с них сеансов связи[3].

---

[1] Телемати́ческие службы — службы электросвязи, за исключением телефонной, телеграфной служб и службы передачи данных, предназначенные для передачи информации через сети электросвязи (см.: приказ Минсвязи России от 23 июля 2001 г. № 175 «Об утверждении руководящего документа отрасли “Телематические службы”»).

[2] Российская газета. 2000. 29 авг.

[3] Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского. 4-е изд., перераб. и доп. М.: ИНФРА-М, 2018. С. 354.

Форма проведения рассматриваемого ОРМ является исключительно негласной. Она ограничивает конституционные права человека и гражданина на тайну переписки и иных сообщений, передаваемых по компьютерным сетям, а также на тайну частной жизни, содержащейся в банках и базах данных. В связи с этим при истребовании информации, находящейся в ведении операторов связи, ПКИ проводится на основании соответствующих *судебных решений* на ограничение тайны связи[1].

Вместе с тем А.В. Чуркин отмечает частный случай, когда искомая компьютерная информация может быть получена и без судебного решения либо без вынесения об этом компетентным руководителем оперативно-розыскного органа мотивированного постановления. Например, в ситуации, когда подозреваемый непосредственно задержан с поличным на месте совершения преступления в общественном или ином месте, и оперативник осматривает его личное техническое средство (компьютер, смартфон, планшет или другое аналогичное устройство)[2].

Сбор компьютерной информации из открытых источников (получение общедоступной информации) также не требует судебного решения, но он и не относится к ПКИ, а представляет собой наведение справок или его автоматизированную разновидность «информационный поиск».

Юридические условия осуществления ПКИ, как общеобязательные, так и экстраординарные, аналогичны тем, которые свойственны ПТП и СИТКС.

Общеобязательными условиями ПКИ являются:

1) наличие оперативной информации, предусмотренной ч. 2 ст. 8 ФЗ об ОРД;

2) получение судебного решения для начала проведения данного ОРМ (ч. 2 ст. 8 ФЗ об ОРД) и продления срока его осуществления (ч. 6 ст. 9 ФЗ об ОРД);

3) наличие документально оформленного задания оперативного подразделения (в форме мотивированного постановления, утверж-

---

[1] См.: Об отказе в принятии к рассмотрению жалобы гражданина Тарасова Николая Алексеевича на нарушение его конституционных прав частью первой статьи 176 и частью первой статьи 285 Уголовно-процессуального кодекса Российской Федерации: Определение Конституционного Суда РФ от 8 апреля 2010 г. № 433-О-О. П. 2.

[2] *Чуркин А.В.* Некоторые правовые аспекты проведения оперативно-разыскного мероприятия «Получение компьютерной информации» // Оперативник (Сыщик). 2018. № 2 (55). Апрель. М.: Издательский дом Шумиловой И.И., 2018. С. 28–34.

денного соответствующим руководителем) для специализированного подразделения;

4) проведение указанного мероприятия с использованием оперативно-технических сил и средств исключительно органов федеральной службы безопасности или органов внутренних дел (ч. 4 ст. 6 ФЗ об ОРД);

5) запрет на проведение ПКИ по основаниям, предусмотренным пп. 1–4 и 6 ч. 2 ст. 7 ФЗ об ОРД, в целях осуществления оперативно-проверочной работы. Исключением является возможность его проведения для обеспечения собственной безопасности органов, осуществляющих ОРД (п. 5 ч. 2 ст. 7 ФЗ об ОРД).

Условиями для экстренного проведения ПКИ (согласно ч. 3 ст. 8 ФЗ об ОРД) являются:

а) наличие обстоятельств, которые не терпят отлагательства и могут привести к совершению тяжкого или особо тяжкого преступления;

б) получение данных о событиях и действиях (бездействии), создающих угрозу безопасности Российской Федерации.

В этих ситуациях предусмотрено:

1) оформление мотивированного постановления руководителя органа, осуществляющего ОРД;

2) наличие документально оформленного задания для осуществления указанного мероприятия специализированными подразделениями;

3) уведомление в течение 24 часов о начале проведения данного мероприятии суда (судьи);

4) при необходимости продолжения ПКИ — получение инициатором указанного ОРМ в течение 48 часов с момента его начала соответствующего судебного решения.

В качестве *субъектов* ПКИ рассматриваются:

- сотрудники оперативных подразделений государственных органов, уполномоченных на осуществление ОРД, — инициаторы задания;
- сотрудники федеральной службы безопасности и органов внутренних дел, которые осуществляют названное ОРМ по заданиям оперативных подразделений как самостоятельно, а также путем конспиративного подключения к станционной аппаратуре операторов связи;
- операторы связи, которые по требованию органов федеральной службы безопасности обязаны включать в состав аппаратных средств дополнительные оборудование и программные средства и создавать другие условия, необходимые для проведения ОТМ.

Профессор А.Ю. Шумилов наряду с ними в качестве дополнительных субъектов рассматривал также руководителя оперативно-розыскного органа, утверждающего задание на проведение ПКИ, судью, который санкционирует его проведение, а также специалиста по компьютерной информации, оказывающего помощь при проведении данного ОРМ[1].

Передача предприятиями, организациями и учреждениями, оказывающими услуги по предоставлению сведений из информационных систем (банков данных) с использованием технических каналов связи заинтересованным оперативным подразделениям, содержанием рассматриваемого ОРМ не охватывается. В этом случае речь также следует вести о наведении справок.

Объектами ПКИ являются:

1) лица, подготавливающие, совершающие или совершившие преступное деяние, по которому производство предварительного следствия обязательно;

2) случайные лица, не относящиеся к криминальной среде, контактирующие с объектами ПКИ по техническим каналам передачи компьютерной информации.

Предметом ПКИ является компьютерная информация, передаваемая по контролируемым техническим каналам связи.

Абсолютно прав профессор А.Л. Осипенко, который отмечает, что получение оперативно значимой компьютерной информации предполагает, в частности, обследование информационных объектов сети Интернет, среди которых следует выделить:

а) закрытые информационные ресурсы, содержащие сведения о совершении преступлений и лицах, их совершающих (сайты криминальных структур, через которые распространяется социально опасная информация, реализуются предметы, запрещенные к обороту, ведется пропаганда криминального образа жизни, вовлекаются в противоправную деятельность новые участники и т.п.);

б) места сетевого общения (закрытые сетевые форумы и чаты, сообщества криминальной направленности в социальных сетях и др.) криминально настроенных лиц и их персональные страницы в социальных сетях. Оперативно значимая информация на указанных объектах может концентрироваться в виде следов противоправной деятельности, ссылок на материалы, запрещенные к рас-

[1] Основы оперативно-разыскной деятельности: учебник: в 2 т. Т. 1. Общая часть / С.П. Жданов, О.Г. Карпович, Е.С. Недосекова [и др.]; предисл. В.Б. Мантусова; под ред. А.Ю. Шумилова. Люберцы: РИО Российской таможенной академии, 2020. С. 255.

пространению, сообщений лиц, осведомленных об обстоятельствах подготовки и совершения преступлений.

Среди источников получения оперативно значимой компьютерной информации, по мнению указанного автора, особое место занимают сетевые каналы коммуникации, задействованные преступниками для координации действий с использованием электронной почты, средств обмена сообщениями, приложений VoIP (интернет-телефонии), мессенджеров и т.п. Обнаружение и контроль таких каналов оперативными подразделениями обеспечивает им существенные преимущества. При этом важно учитывать, что количество сетевых сервисов, устанавливающих текстовую, голосовую и видеосвязь между компьютерами через интернет, постоянно увеличивается (ICQ, Skype, WhatsApp, Viber, Telegram и др.), причем многие из них предоставляют услуги шифрования передаваемых данных[1].

Следует учитывать, что спектр технических источников оперативно значимой компьютерной информации в ближайшее время будет расширяться и за счет новых видов так называемых «умных вещей», оснащенных микропроцессорами и способных осуществлять обмен данными с телекоммуникационными сетями (навигационные системы автотранспорта, системы «умного дома», «умные» бытовые приборы, информационные датчики в местах общественного пользования и т.п.). Смена в современном обществе концепции «Интернета вещей» на «Интернет всего» предполагает подключение к сети практически всех объектов и инфраструктур, обслуживающих интересы как отдельных граждан, так и общества в целом[2].

Место проведения ПКИ в Законе не определено. По аналогии с ПТП и СИТКС в качестве такового следует рассматривать помещения, занимаемые операторами компьютерной связи, а также помещения специализированных подразделений органов федеральной службы безопасности и органов внутренних дел, занимающихся осуществлением данного ОТМ.

ПКИ может являться продолжаемым, длительным по времени мероприятием. *Срок его проведения* может составлять до 180 суток со дня вынесения судебного решения. При необходимости про-

---

[1] Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского. 4-е изд., перераб. и доп. М.: ИНФРА-М, 2018. С. 353.

[2] *Ваннах М.* Через Интернет вещей — к Интернету всего // Компьютерра. URL: https://www.computerra.ru/183215/cherez-internet-veshhey-k-internetu-vsego/ (дата обращения: 26.06.2020).

дления срока действия постановления судья выносит судебное решение на основании вновь представленных материалов. Как и при проведении других ОТМ, располагая данными о конкретных сроках поступления интересующей его информации, инициатор вправе провести в этот период ПКИ *разового* характера. При этом течение срока вынесенного решения не прерывается.

Контроль за циркулирующей в контролируемых сетях информацией, которая содержит сведения, составляющие *государственную тайну*, допускается только при условии соблюдения режима секретности.

Полученные в ходе ПКИ данные *оформляются* рапортом, справкой или актом специализированного подразделения, а также объяснениями (заявлениями) лиц, участвовавших в проведении данного мероприятия. К оперативно-служебным документам приобщается полученная компьютерная информация в виде *файлов*, представляющих собой последовательный набор данных, хранящийся на определенном физическом носителе и имеющий собственные имя и расширение.

Полученные результаты ОРД вводятся в уголовный процесс путем допроса сотрудников оперативных подразделений, инициировавших данное мероприятие, и иных лиц, принимавших участие в его осуществлении (за исключением сотрудников ОТП и конфидентов), осмотра представленных носителей компьютерной информации и их приобщения к делу в качестве вещественных доказательств.

Привести подробное описание всех особенностей практического осуществления ОРМ «получение компьютерной информации» в настоящее время не представляется возможным, поскольку, как уже подчеркивалось, пока отсутствует нормативное толкование содержания данного мероприятия, и в достаточной мере не наработана практика его применения. Между тем потенциал применения ПКИ в решении задач ОРД, несомненно, весьма высок. Самые серьезные перспективы оно открывает в сочетании с использованием в обработке получаемой компьютерной информации особых технологий анализа так называемых «больших данных» (BigData), позволяющих производить сбор максимально полной информации об объектах оперативного интереса с формированием «электронного досье» на потенциальных преступников, обнаружением и визуализацией их неявных связей с иными объектами и событиями криминального характера, выявлением группировок криминальной направленности и установлением их специализации, степени организованности, распределения ролей, причастности фи-

гурантов к тем или иным событиям. Более того, анализ «больших данных» создает реальную технологическую основу использования оперативно-розыскных методов для прогнозирования социально опасных событий и предупреждения преступлений за счет обнаружения «цифровых следов» с заданными свойствами, указывающими на высокую вероятность подготовки либо совершения определенных криминальных деяний.

Еще одним резервом повышения эффективности ПКИ призвано послужить внесение в ФЗ об ОРД изменений и дополнений, разработанных МВД России, которые направлены на совершенствование деятельности по пресечению преступлений с использованием информационно-телекоммуникационных технологий.

Специалисты отмечают, что в 2020 г. около 25% всех совершенных преступлений так или иначе были связаны с использованием средств электронно-вычислительной техники. Причем на протяжении последних лет число киберпреступлений неуклонно возрастает. В отчетном периоде оно увеличилось на 73,4%, в том числе с использованием сети Интернет — на 91,3%, а при помощи средств мобильной связи — на 88,3%. Вместе с тем до суда удается довести лишь сравнительно небольшое количество возбуждаемых уголовных дел (в 2020 г. — всего 16%)[1].

Руководство МВД России полагает, что причиной такого положения дел является отсутствие достаточных оперативных возможностей, связанных с документированием киберпреступлений после получения компьютерной информации. Полицейские сталкиваются с серьезными трудностями в случае использования злоумышленниками так называемых удаленных рабочих столов. Подобные возможности позволяют дистанционно уничтожать любые компьютерные данные из облачного хранилища на удаленном сервере. На практике это зачастую приводит к утрате части доказательной базы, даже в случае изъятия в рамках ПКИ используемых средств коммуникации.

Законопроект предполагает внесение в перечень ОРМ, предусмотренный ч. 1 ст. 6 ФЗ об ОРД, нового ОРМ — «*исследование компьютерной информации*», которое позволит «оперативно исследовать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, в том числе с привлечением квалифицированных

[1] Краткая характеристика состояния преступности в Российской Федерации за январь — декабрь 2020 года // Официальный сайт МВД России. URL: https://мвд.рф/reports/item/22678184/ (дата обращения: 29.05.2021).

специалистов, на предмет установления следов преступления, совершенного с использованием информационных технологий, и их закрепления в качестве вещественных доказательств по уголовным делам».

Организация и тактика проведения данного ОРМ должны быть определены органами, осуществляющими ОРД, с учетом их ведомственной специфики[1].

В связи с рассмотренной выше законодательной инициативой МВД России следует высказать еще одно суждение, связанное с оптимизацией ПКИ. Оно касается использования для поиска и исследования компьютерной информации логико-аналитических систем, основанных на применении ИИ.

---

[1] Разработаны поправки в закон «Об оперативно-розыскной деятельности» // Юридическая социальная сеть. 2021. 29 мая. URL: https://www.9111.ru/questions/7777777771337697/ (дата обращения: 29.05.2021).

А.А. Бабушкин

Формирование системы оперативно-розыскного контроля органов внутренних дел за лицами, склонными к совершению преступлений, в условиях развития информационного общества

В течение последних двух десятилетий происходит интенсивное развитие информационных, коммуникационных и поведенческих технологий, что существенно меняет условия, в которых оперативные подразделения ОВД выполняют возложенные на них задачи. К настоящему времени организованная преступность, террористические организации, враждебно настроенные государства и иные деструктивные силы наиболее активно и умело научились использовать возникший разрыв между удобством и безопасностью ИКТ.

Одним из ключевых приоритетов национальной безопасности Российской Федерации, неотъемлемым компонентом которой выступает информационная безопасность, является существенное сокращение, а в перспективе и ликвидация указанного пробела. Это относится и к киберпространству, и шире — к информационной среде, охватывающей всю совокупность сообщений, знаний, новостей и т.п., все чаще используемых в деструктивных и враждебных целях, включая применение информационных технологий в качестве оружия[1].

Показывает свою эффективность превентивная парадигма сдерживания, при которой вся политика национальной безопасности той или иной страны и обеспечивающие ее выполнение компоненты ориентированы на раннее распознавание рисков, угроз и факторов, угрожающих интересам государства, общества и граждан во всех пяти сферах противоборства: на земле, в воздухе, под водой, в космосе и в киберпространстве. Следует отметить, что и в нашей стране приоритет предотвращения компьютерных атак в качестве одного из принципов обеспечения безопасности критической информаци-

[1] См.: *Маслов А.А.*, *Бабушкин А.А.* Формирование правовых основ оперативно-розыскного обеспечения коллективной безопасности // Общество и право: научно-практический журнал. 2020. № 1 (71). С. 50–59.

онной инфраструктуры нашел законодательное закрепление (ст. 4 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

Указанные тенденции следует рассматривать в качестве определяющих факторов при формировании принципиально новой системы оперативно-розыскного контроля органов внутренних дел (далее — ОРК ОВД) за лицами, склонными к совершению преступлений, которая должна быть органически вплетена в единую систему государственных мер противодействия и сдерживания преступности, терроризма и иных угроз как в физической, так и в виртуальной среде.

При этом формирование данной системы должно осуществляться в соответствии с положениями и принципами, заложенными руководством страны в таких документах, как Стратегия национальной безопасности Российской Федерации[1], Стратегия развития информационного общества в Российской Федерации на 2017–2030 годы[2], Национальная стратегия развития искусственного интеллекта на период до 2030 года[3] и ряде других, в целях повышения эффективности ОРД, ее перехода на качественно новый уровень, адекватный характеру современных криминальных угроз.

Говоря об ОРК ОВД за лицами, склонными к совершению преступлений, мы в первую очередь имеем в виду деятельность оперативных подразделений полиции по обеспечению реализации такой важной меры предупреждения и профилактики преступлений, как административный надзор. Это обусловлено тем, что на сегодняшний день согласно действующему законодательству лишь установление в отношении лица административного надзора дает основания для участия оперативных подразделений ОВД в осуществлении контроля за поведением лиц, находящихся в «группе риска», когда отсутствуют сведения о конкретных фактах их преступной деятельности.

Вместе с тем границы такого участия законодательно четко не определены, что не позволяет задействовать при осуществлении контроля за поднадзорными лицами весь комплекс оперативно-розыскных методов, сил и средств. Это обстоятельство ставит на повестку дня вопрос формирования правовой основы ОРК ОВД за лицами, склонными к совершению преступлений, которая бы

---

1 Утверждена Указом Президента РФ от 2 июля 2021 г. № 400.

2 Утверждена Указом Президента РФ от 9 мая 2017 г. № 203.

3 Утверждена Указом Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

полностью соответствовала современным социально-правовым условиям развития информационного общества и обеспечивала упреждающее реагирование на криминальные угрозы.

Фактическое отсутствие административного надзора как меры превентивного воздействия на лиц, склонных к совершению преступлений, с начала 1990-х гг. до принятия Федерального закона от 6 апреля 2011 г. № 64-ФЗ «Об административном надзоре за лицами, освобожденными из мест лишения свободы» (далее — ФЗ об административном надзоре) можно считать негативным историческим примером отступления от политики наступательного (упреждающего) противодействия преступности, в первую очередь ее наиболее опасным организованным формам, когда в приоритет ставятся выявление и раскрытие уже совершенных преступлений, а не их предупреждение и профилактика.

Административный надзор представляет собой осуществляемое ОВД наблюдение за соблюдением лицом, освобожденным из мест лишения свободы, установленных судом временных ограничений его прав и свобод, а также за выполнением им обязанностей, предусмотренных законодательством (ст. 1 ФЗ об административном надзоре).

При этом задачами административного надзора являются предупреждение совершения поднадзорными лицами преступлений и других правонарушений и оказание на них индивидуального профилактического воздействия в целях защиты государственных и общественных интересов.

Изучение уголовных дел и оперативных материалов позволяет сделать обоснованный прогноз о дальнейшей активизации участия представителей организованной преступности, ядро которой составляют ранее судимые, в противоправной деятельности, осуществляемой с использованием ИКТ. Ее организаторы и активные участники готовы продолжать свой криминальный промысел после освобождении из мест лишения свободы. Кроме того, известны случаи использования знаний и навыков данных лиц лидерами и авторитетами уголовно-преступной среды непосредственно в исправительных учреждениях.

С учетом динамики выявления преступлений, совершаемых с использованием ИКТ, можно прогнозировать значительное увеличение доли лиц, их совершивших, среди ранее судимых, состоящих на профилактическом учете. В целях предупреждения совершения ими новых преступлений необходимо установление постоянного контроля за их поведением после освобождения из мест

лишения свободы, в том числе с использованием возможностей административного надзора.

При этом необходимо учитывать, что ныне действующая система административных запретов и ограничений, связанная в основном с обязательным нахождением в ночное время суток поднадзорных лиц по месту жительства (пребывания) и периодической явкой на регистрацию в территориальный ОВД, для данной категории фигурантов явно недостаточна.

Представляется, что в современных условиях перемещения значительного сегмента преступности в цифровую среду институт административного надзора может быть эффективным только в случае расширения полномочий оперативных подразделений полиции в части предоставления им возможности осуществлять постоянный (в том числе негласный) контроль за используемой поднадзорными лицами компьютерной и иной техникой, средствами связи, а также проводить скрытое визуальное или электронное наблюдение за их поведением в местах проживания и притяжения.

В настоящее время ВНИИ МВД России совместно с заинтересованными подразделениями центрального аппарата подготовлен проект дополнений в Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности» (далее — ФЗ об ОРД), существенно расширяющих полномочия оперативных подразделений в сфере предупреждения рецидивной преступности, а также предусматривающих изменение сроков хранения материалов, полученных в результате проведения ОРМ в отношении лиц, занимающих высшее положение в преступной иерархии.

На наш взгляд, в процессе оперативно-розыскного обеспечения административного надзора, помимо предупреждения преступлений, должны решаться и иные задачи, предусмотренные ст. 2 ФЗ об ОРД. В первую очередь речь идет о пресечении, выявлении и раскрытии преступлений, совершаемых или совершенных поднадзорными лицами, и их связей.

По этой причине в ст. 2 ФЗ об административном надзоре («Задачи административного надзора») целесообразно предусмотреть, что административный надзор устанавливается для противодействия противоправной деятельности поднадзорных лиц (а не только для предупреждения совершения ими преступлений, как в действующей редакции), а также оказания на них индивидуального профилактического воздействия.

Для усиления оперативно-розыскной составляющей, без которой рассматриваемый институт не может быть эффективным, ст. 12 ФЗ об административном надзоре («Полномочия органов внутренних

дел по осуществлению административного надзора») необходимо дополнить положением, согласно которому в отношении поднадзорного лица разрешается проводить ОРМ в порядке, предусмотренном законодательством Российской Федерации.

При этом следует согласиться с теми авторами, которые в целях повышения эффективности противодействия преступлениям, совершаемым с использованием ИТТ, предлагают нормативно закрепить на ведомственном уровне право сотрудников оперативных подразделений ОВД в рамках ОРМ «наведение справок» использовать различные мобильные приложения, интернет-сервисы и программное обеспечение, применение которых не требует наличия специальных технических знаний, при условии соблюдения принципа конспирации[1]. Полагаем, что активное использование данных информационных технологий, не требующее специальной технической подготовки, в процессе осуществления административного надзора существенно повысит его превентивный потенциал.

Федеральным законом от 23 июня 2016 г. № 182-ФЗ «Об основах системы профилактики правонарушений в Российской Федерации» определено, что одним из основных направлений осуществления профилактики правонарушений является развитие системы профилактического учета лиц, склонных к совершению правонарушений, который предназначен для информационного обеспечения деятельности субъектов профилактики (ст. 6).

Согласно ст. 17 рассматриваемого Федерального закона одной из форм профилактического воздействия является профилактический надзор, который состоит в наблюдении за поведением лица, состоящего на профилактическом учете, и соблюдением им ограничений, установленных в соответствии с законодательством Российской Федерации (ст. 23).

Реализация основных направлений профилактики правонарушений осуществляется посредством применения в соответствии с законодательством Российской Федерации специальных мер профилактики правонарушений административного, уголовного, уголовно-процессуального, уголовно-исполнительного и оперативно-розыскного характера.

Важно отметить, что профилактический и административный надзор — различные институты, имеющие разное правовое содер-

[1] См.: *Демин Ю.В.* Организационно-правовые основы выявления и раскрытия краж, совершаемых с банковского счета, а равно в отношении электронных денежных средств // Российский следователь: научно-практическое и информационное издание. 2021. № 1. С. 64–68.

жание, хотя и тесно взаимосвязанные. Очевидно, что установление административного надзора в отношении лица влечет более серьезные ограничения и запреты. Даже оперативно-розыскное обеспечение административного надзора, снабженное хоть какими-то организационно-правовыми механизмами, фактически находится на стадии формирования. По этой причине говорить об оперативно-розыскном обеспечении профилактического надзора, осуществляемого участковыми уполномоченными полиции, как минимум преждевременно. Напомним, что помимо поднадзорных лиц объектами профилактического надзора являются все ранее судимые, условно осужденные, условно-досрочно освобожденные и иные лица. Их общее количество по стране ежегодно составляет более полумиллиона.

В связи с этим существенное значение для обеспечения эффективного ОРК ОВД имеет организация совместно с подразделениями ФСИН России наблюдения за осужденными, которым назначено наказание, не связанное с изоляцией от общества.

Федеральным законом от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» УИК РФ был дополнен ст. 18.1 («Объявление розыска и осуществление оперативно-розыскной деятельности при исполнении наказаний, не связанных с изоляцией осужденных от общества»), в соответствии с которой ОРД при исполнении наказаний, не связанных с изоляцией осужденных от общества, осуществляется оперативными подразделениями уголовно-исполнительной системы самостоятельно, оперативными подразделениями уголовно-исполнительной системы во взаимодействии с оперативными подразделениями иных государственных органов, определенных ФЗ об ОРД, в пределах их компетенции и оперативными подразделениями иных государственных органов, определенных указанным Федеральным законом, в пределах их компетенции.

Вместе с тем на сегодняшний день отсутствуют законодательные основания для проведения ОРМ в отношении данной категории лиц, за исключением случаев, когда имеются сведения о конкретных подготавливаемых, совершаемых или совершенных ими преступлениях (ч. 1 ст. 7 ФЗ об ОРД).

Таким образом, использование ИТТ в процессе ОРК ОВД за лицами, склонными к совершению преступлений, приобретает особую актуальность в связи с отсутствием законодательных оснований для проведения ОРМ в отношении поднадзорных лиц и иных лиц, состоящих на профилактических учетах и находящихся в «группе

риска». Это обусловлено тем, что современные ИТТ позволяют получать оперативно-значимую информацию в рамках правового поля даже без проведения специальных технических мероприятий. В частности, для этих целей можно широко использовать изучение профилей фигурантов в социальных сетях и различных приложениях. Большую помощь в осуществлении оперативно-розыскного обеспечения административного надзора могут оказать системы видеонаблюдения, в первую очередь АПК «Безопасный город».

Система ОРК ОВД должна быть ориентирована на формирование и развитие технологических основ непрерывного мониторинга и контроля в сфере борьбы с преступностью. Важная роль в этом процессе отведена так называемым технологиям распознавания и идентификации (биометрические, аудиологические, оптические и др.), которые позволяют устанавливать лиц, подозреваемых в совершении преступлений, находящихся в розыске, а также представляющих оперативный интерес, с помощью систем фото- и видеофиксации, отслеживать их перемещения и действия как в режиме реального времени, так и ретроспективно.

Электронные устройства генерируют новые данные с невероятной скоростью. Значительная часть данных может быть использована для профилактики преступности. Если раньше общественность интересовали прежде всего процедуры доступа к персональным и корпоративным данным, то в ближайшие годы необходимо, не дожидаясь кризиса общественного мнения, четко регламентировать доступ правоохранительных структур к потоковым видеоданным, протоколам платежных систем и, конечно же, протоколам «Интернета вещей». Уже сегодня данные, получаемые со смартфонов, в том числе пространственно-временная информация, позволяют раскрыть и предотвратить многие особо опасные преступления.

Конечная задача состоит в том, чтобы сотрудники оперативных подразделений полиции смогли получать необходимую информацию в полном объеме в режиме реального времени в удобном и доступном для практического использования виде.

Надо стремиться к тому, чтобы российская полиция в новых условиях осуществила перевод своей оперативно-служебной деятельности на новую технологическую платформу, что позволит ее оперативным подразделениям:

- все шире и с бóльшими результатами переходить от раскрытия и пресечения к профилактике (раннему предупреждению) преступлений (в ряде зарубежных государств уже появился соот-

ветствующий термин — «предиктивная полицейская деятельность»);

- использовать информацию, поступающую не только из баз данных ОВД, но и от других государственных и частных структур, что позволит действовать упреждающе и своевременно выявлять лиц, группы и организации, наиболее уязвимые для преступников;
- на ранней стадии распознавать подозрительные модели деятельности и следы готовящихся преступлений (наибольший эффект здесь может дать совмещение аналитики электронных платежей с видеоаналитикой и аналитикой совершаемых покупок).

Оперативно-розыскная информация представляет собой сведения о лицах, предметах, событиях, явлениях и процессах, независимо от формы их представления, которые используются в целях получения знаний, имеющих значение для решения задач борьбы с преступностью. В то же время имеются огромные пласты исследований, в которых обстоятельно рассмотрены самые различные аспекты, отражающие многогранность и исключительное значение для правоохранительной деятельности оперативно-розыскной информации[1].

Участковые уполномоченные, сотрудники подразделений по организации административного надзора и по делам несовершеннолетних осуществляют профилактическую деятельность и заводят дела профилактического учета, в которых концентрируется информация о криминальной активности подучетных лиц и их связях, которая может быть использована для решения как задач ОРК, так и ОРД в целом.

В целях ее аналитической обработки и своевременного реагирования на содержащиеся в ней сведения о замышляемых, подготавливаемых, совершаемых или совершенных преступлениях необходимо, чтобы она на системной основе поступала в единую базу данных оперативно-розыскного назначения в рамках профилактических информационных потоков с пометкой «для служебного пользования» либо в открытом кодированном виде.

Как справедливо отмечено С.С. Овчинским, прогностические методики с точки зрения задач ОРД призваны обеспечить обнаружение наиболее активных очагов возникновения преступности. В силу этого осуществляемая на основе прогностической инфор-

[1] См.: Оперативно-розыскная деятельность / под ред. К.К. Горяинова, В.С. Овчинского, А.Ю. Шумилова. М.: ИНФРА-М, 2001; *Яковец Е.Н.* Основы информационно-аналитического обеспечения оперативно-розыскной деятельности. М.: Щит-М, 2009.

мации «выборка» из круга лиц, повседневно попадающих в поле зрения полиции, а также из числа освобождаемых из мест лишения свободы тех, у кого отклоняющееся от норм поведение может развиться в преступное, должна быть научно обоснованной, лишенной субъективизма, предвзятости и формализма, которые невольно довлеют над практикой, в частности, в силу больших «допусков», содержащихся в нормативных актах, регламентирующих этот сложный процесс. Неэффективность индивидуально-профилактических и оперативно-розыскных мер борьбы с преступностью как раз и объясняется «попаданием мимо цели» в тех случаях, когда выявляют лиц, представляющих оперативный интерес[1].

Чтобы иметь необходимый предупредительный (предиктивный) эффект, данная информация должна соотноситься с личностью фигуранта, оцениваться с позиции ее потенциальной общественной опасности, перепроверяться через иные источники и доводиться до компетентных оперативных подразделений ОВД в качестве выводов. Все это должно осуществляться непрерывно на системной основе в рамках соответствующих информационно-аналитических подсистем и цифровых досье.

Соотнесение имеющейся оперативно-розыскной информации с личностными характеристиками лиц, в отношении которых заведены профилактические цифровые досье, ее систематизация и актуализация с целью прояснения преступных намерений и действий позволяют говорить о наличии в распоряжении оперативных аналитиков сведений, являющихся основаниями для проведения в отношении данной категории лиц полного комплекса ОРМ, минуя стадию предварительной оперативной проверки, которая проходит фактически в цифровом виде. Чаще всего данная информация относится к тем лицам, которые уже имеют криминальный опыт. В ней также могут содержаться сведения об условиях, способствующих активизации преступной деятельности лица, либо наоборот — временно ее сдерживающих.

Для развития и совершенствования оперативно-аналитического обеспечения оперативно-профилактического наблюдения целесообразно использовать зарубежный опыт ведения цифровых досье на лиц, представляющих оперативный интерес.

---

[1] *Овчинский С.С.* Оперативно-розыскная информация: монография / под ред. А.С. Овчинского, В.С. Овчинского. 2-е изд., доп. М.: ИНФРА-М, 2017. С. 190.

Так, с 2010 г. в ФБР проходит модернизация деятельности его Информационного центра, включающего 21 базу данных (подсистемы), содержащих досье на 12 млн преступников. Данная информационно-аналитическая система в среднем отвечает на 14 млн запросов в день. Информационный центр ФБР находится на стадии модернизации, его новые помещения будут в 12 раз превосходить старые и иметь в 50 раз больше емкости и мощности хранения и обработки «больших данных». Программно-аппаратная архитектура нового центра проектируется на основе искусственного интеллекта[1].

В Великобритании достаточно подробно описан опыт освоения ИТТ в правоохранительной деятельности. Так, в 2017 г. Королевский институт специальных операций и безопасности Великобритании опубликовал доклад «Большие данные и полиция», в котором подробно обосновывается необходимость переориентирования полиции на предиктивную (предупредительную) деятельность как основную функцию[2].

Развитие британской предиктивной полицейской деятельности осуществляется одновременно с совершенствованием ее информационной основы, что позволило 95% опрошенным офицерам полиции отметить, что их осведомленность на порядок выше, чем у коллег с континента, и позволяет успешно бороться с организованной преступностью.

На проектную мощность вышла общенациональная база данных национальной компьютерной полиции, которая еще в 2017 г. содержала 12,2 млн файлов личных данных на преступников, связанных с ними граждан и приезжих. Данная база тесно взаимодействует с национальной базой полиции, в которой содержатся копии всех местных полицейских записей (начиная с 2015 г. вся полицейская документация ведется в бумажном и электронном или исключительно в электронном виде). В настоящее время в цифровой

---

1 *Овчинский В.С.* Использование искусственного интеллекта в оперативно-аналитической деятельности ФБР по борьбе с преступностью // Актуальные проблемы теории оперативно-розыскной деятельности: сб. науч. тр. М.: ИНФРА-М, 2017. С. 393.

2 *Babuta A.* Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities // RUSI Occasional Paper. September, 2017. URL: https://www.rusi.org/explore-our-research/publications/occasional-papers/big-data-and-policing-assessment-law-enforcement-requirements-expectations-and-priorities (дата обращения: 20.08.2021).

формат переведены все полицейские отчеты за период с начала века, находящиеся в полиции. При таком подходе главный акцент смещается с фиксации и анализа совершенных правонарушений и преступлений на упреждающее прогнозирование и проактивную (превентивную) диагностику индивидуального и группового преступного поведения.

С.И. Давыдов, Е.О. Наливайко

О необходимости введения в научный оборот оперативно-розыскной категории «дистанционное мошенничество»

Понятие дистанционного мошенничества пока еще не относится к числу общепринятых и устоявшихся в оперативно-розыскной теории и практике. Для обозначения преступных деяний, связанных с хищением денежных средств путем обмана, совершаемых в удаленном, дистанционном формате, в настоящее время используются разные термины и словосочетания — «мошенничества, совершаемые с использованием информационно-телекоммуникационных технологий», «мошенничества, совершаемые с использованием сети Интернет», «мошенничества, совершаемые с использованием средств мобильной связи и компьютерной техники»; «кибермошенничества», «IT-мошенничества», «сетевые мошенничества», «онлайн-мошенничества»; «мошенничества, совершенные дистанционным путем» и др. Многочисленность терминов и отсутствие единого подхода к их толкованию явно не способствует формированию профессионального научного языка и оперативно-розыскного мышления. Между тем, как отмечает А.Г. Маркушин, «точность и ясность формулировок определений, четкое их языковое воплощение, правильное и единообразное употребление терминологии выполняют важнейшие коммуникативные и познавательные функции»[1].

В современных условиях распространения киберпреступлений, особенно мошенничества, остро стоит вопрос эффективного методического обеспечения деятельности оперативных подразделений по их выявлению и раскрытию. В связи с этим необходимо определиться с терминами, которые целесообразно использовать при разработке соответствующих оперативно-розыскных методик и которые были бы удобны для применения в оперативно-розыскной практике.

---

[1] *Маркушин А.Г.* О научных проблемах оперативно-розыскной деятельности // Некоторые проблемы оперативно-розыскной деятельности: сб. ст. / под ред. А.А. Фальченко. Н. Новгород, 1996. Вып. 2. С. 11.

Полагаем, что сформировались все предпосылки для того, чтобы ввести в понятийный аппарат оперативно-розыскной науки категорию «дистанционное мошенничество».

В статье предполагается решить следующие задачи:

— исследовать распространенность использования понятия дистанционного мошенничества в уголовном законодательстве, ведомственной нормотворческой деятельности, а также в оперативно-розыскной теории и других науках уголовно-правового цикла;

— выявить оперативно значимые признаки и обосновать понятие дистанционного мошенничества;

— раскрыть значение ввода в научный оборот оперативно-розыскного понятия дистанционного мошенничества.

Анализируя статьи Уголовного кодекса РФ, устанавливающие уголовную ответственность за мошенничество (ст. 159) и его различные виды (ст. 159.1, 159.2, 159.3, 159.4, 159.5, 159.6), мы не находим в их формулировках применительно к описанию объективной стороны преступления термина «дистанционный». Отметим при этом, что в двух из перечисленных статей используются термины, характеризующие мошенничества как совершаемые с использованием информационных технологий. Это ст. 159.3 УК РФ «Мошенничество с использованием электронных средств платежа» и ст. 159.6 УК РФ «Мошенничество в сфере компьютерной информации».

В то же время в ведомственных нормативных актах МВД России термин «дистанционное мошенничество» уже используется, хотя и не так широко. К примеру, в решении коллегии МВД России от 1 ноября 2019 г. № 3 содержатся такие формулировки: «по-прежнему немалая часть так называемых “дистанционных мошенничеств” совершается лицами, отбывающими наказания в местах лишения свободы», «возникает необходимость систематизации в рамках единой базы данных “Дистанционное мошенничество” информации о зарегистрированных IT-преступлениях»[1].

Наряду с этим активно используется термин «дистанционное мошенничество» на официальных сайтах ОВД регионального уровня

[1] Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий»: приказ МВД России от 25 ноября 2019 г. № 878 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=519451#W4WNegSYH3nGzvxY1 (дата обращения: 10.12.2020).

различных субъектов РФ (например, г. Москва и Московская область, Краснодарский край, республики Ингушетия, Башкортостан, Крым и др.), где размещены материалы профилактического характера для населения.

Как показал опрос сотрудников оперативных подразделений, более 90% из них считают, что использование в повседневной деятельности термина «дистанционное мошенничество» является сегодня достаточно распространенным.

Обосновывая целесообразность введения в понятийный аппарат категории «дистанционное мошенничество», будет правильным представить результаты изучения научных трудов, где используется указанное понятие. Надо сказать, что обращение ученых к термину «дистанционное мошенничество» или к каким-то другим схожим по смыслу словосочетаниям, например «мошенничество, совершенное дистанционным способом», становится все более частым.

К примеру, В.Ф. Васюков в своей докторской диссертации закрытого характера (2018 г.), посвященной раскрытию и расследованию преступлений с использованием информации из систем сотовой связи, термин «дистанционный» использует неоднократно, в том числе характеризуя хищения, совершаемые с использованием информационно-телекоммуникационных технологий.

Можно привести немало научных публикаций по криминалистике, криминологии, уголовному праву и уголовному процессу, где используется понятие «дистанционное мошенничество». Выделим лишь некоторых авторов таких работ. Это Ф.А. Абашева и К.П. Гришкина[1], А.В. Богданов, И.И. Ильинский и В.Е. Хазов[2], В.О. Давыдов и И.В. Тишутина[3], Н.Д. Литвинов и А.Н. Федоров[4],

[1] *Абашева Ф.А., Гришкина К.П.* Дистанционные мошенничества как одна из проблем посягательств на основы конституционного строя и безопасности государства: понятие и особенности расследования // 25 лет Конституции Удмуртской Республики: итоги и перспективы развития: сб. ст. Ижевск, 2020. С. 9–17.

[2] *Богданов А.В., Ильинский И.И., Хазов В.Е.* Киберпреступность и дистанционное мошенничество как одна из угроз современному обществу // Криминологический журнал. 2020. № 1. С. 15–20.

[3] *Давыдов В.О., Тишутина И.В.* Цифровые следы в расследовании цифрового мошенничества // Известия Тульского государственного университета. Экономические и юридические науки. 2020. № 3. С. 20–27.

[4] *Литвинов Н.Д., Федоров А.Н.* Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // Научно-исследовательские публикации. 2015. № 12. С. 73–80.

А.А. Лебедева[1], Я.М. Мазунин и К.С. Сидорова[2], Р.Н. Морозов и В.М. Остапенко[3], А.Р. Напсоков[4], С.В. Петрикова и А.А. Лаврушкина[5], В.А. Рыжак[6], Т.Н. Семенихина[7], П.Л. Сердюк[8], А.А. Хайдаров[9].

В ряде публикаций указанных авторов содержатся объяснения, смысл которых сводится к тому, что активное применение информационно-телекоммуникационных технологий при совершении

---

1 *Лебедева А.А.* Особенности взаимодействия следователя и сотрудников оперативных подразделений при расследовании преступлений в сфере дистанционного мошенничества // Процессуальные и организационно-правовые особенности взаимодействия органов предварительного расследования с органами, осуществляющими оперативно-разыскную деятельность: проблемы и пути их решения: мат-лы междунар. науч.-практич. конф. / под общ. ред. А.М. Багмета. М.: Московская академия СК России, 2018. С. 124–126; *Лебедева А.А.* Способы совершения дистанционного мошенничества в местах лишения свободы // Уголовное судопроизводство: проблемы теории и практики. 2020. № 1. С. 50–53.

2 *Мазунин Я.М., Сидорова К.С.* Следственные ситуации и алгоритм их разрешения при расследовании мошенничеств, совершаемых дистанционным способом в современных условиях // Технологии XXI века в юриспруденции: мат-лы Второй междунар. науч.-практич. конф. / под ред. Д.В. Бахтеева. Екатеринбург, 2020. С. 465–470.

3 *Морозов Р.Н., Остапенко В.М.* Особенности преодоления противодействия, осуществляемого подозреваемыми (обвиняемыми) на первоначальном этапе расследования дистанционных мошенничеств, совершенных в пенитенциарных учреждениях // Юридические науки. 2019. Т. 13. № 4. С. 543–552.

4 *Напсоков А.Р.* Проблемы организации деятельности по раскрытию дистанционных мошенничеств и краж с банковских карт // Пробелы в российском законодательстве. 2020. Т. 13. № 4. С. 262–264.

5 *Петрикова С.В., Лаврушкина А.А.* Некоторые объективные признаки дистанционного мошенничества // Законодательство. 2019. № 5. С. 62–68.

6 *Рыжак В.А.* Проблемы теории и практики расследования дистанционного мошенничества // Уголовное судопроизводство России: проблемы и перспективы развития: сб. мат. Всерос. науч.-практич. конф. М., 2020. С. 191–193.

7 *Семенихина Т.Н.* Особенности проведения осмотра места происшествия при проверке заявления (сообщения) о дистанционном мошенничестве // Гуманитарные, социально-экономические и общественные науки. 2020. № 7. С. 184–186.

8 *Сердюк П.Л.* Особенности правовой оценки дистанционного мошенничества // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2019. № 4 (48). С. 226–230.

9 *Хайдаров А.А.* Дистанционное мошенничество. Расследование преступления и доказывание в суде // Уголовный процесс. 2020. № 10 (190). С. 24–35.

хищений обусловило появление термина «дистанционное мошенничество», предполагающего существенное изменение механизма традиционного вида преступления за счет нивелирования непосредственного контакта преступника с жертвой[1].

Изложенное выше позволяет сделать вывод, что термин «дистанционное мошенничество» используется в научных публикациях достаточно широко, поскольку является наиболее удачным для обозначения особого вида специфических мошеннических действий, связанных с использованием информационно-телекоммуникационных технологий при отсутствии физического контакта преступника с потерпевшим.

При решении задачи определения научного понятия дистанционного мошенничества будем придерживаться изложенных в методологической литературе требований, которым оно должно соответствовать. В.М. Сырых определяет их следующим образом:

— понятие должно «отражать действительные, реальные признаки явлений и процессов и не приписывать им несуществующие свойства, элементы, связи;

— охватываемые понятием признаки должны принадлежать непосредственно отражаемому предмету, процессу, а не каким-либо другим явлениям, процессам;

— признаки должны быть существенными, а не случайными;

— признаки должны быть достаточными для безошибочного отличения предмета, процесса от всех иных сходных с ними предметов и процессов;

— признаки должны быть общими для всего класса предметов, а не какой-либо их части;

— содержание понятия носит конкретно-исторический характер и может меняться по мере развития, совершенствования отражаемого им предмета, процесса»[2].

Важно подчеркнуть, что перед нами не стоит задача раскрыть уголовно-правовую характеристику разных видов мошенничества, совершаемых дистанционных способом, представить элементы состава преступления и проблемы его квалификации. Это задача специалистов в области уголовного права. Мы определяем для себя цель — выявить те признаки мошенничества, совершаемого дистан-

---

[1] См., например: *Давыдов В.О., Тишутина И.В.* Цифровые следы в расследовании цифрового мошенничества // Известия Тульск. гос. ун-та. Экономические и юридические науки. 2020. № 3. С. 21.

[2] *Сырых В.М.* Логические основания общей теории права. Т. 2. Логика правового исследования (Как написать диссертацию). М.: Юстицинформ, 2004. С. 335.

ционным способом, которые имеют оперативно-розыскное значение и определяют особенности деятельности по его выявлению и раскрытию оперативно-розыскными средствами и методами.

Конструирование понятия дистанционного мошенничества как оперативно-розыскной научной категории начнем с анализа значений общеупотребительного слова «дистанционный». В Толковом словаре С.И. Ожегова оно означает «совершаемый на расстоянии»[1]. В Большой Российской Энциклопедии раскрывается технический аспект термина «дистанционное управление», однако смысл тот же — это «управление на расстоянии техническими объектами, при котором для осуществления управляющих воздействий используются специальные средства (системы) передачи воздействий...»[2].

Достаточно интересной представляется трактовка дистанционного мошенничества практиков — сотрудников оперативных подразделений. К примеру, руководитель отдела, специализирующегося на раскрытии указанного вида преступлений УУР ГУ МВД по Алтайскому краю, Е.С. Прохоров в одном из интервью еженедельнику «Аргументы и факты» дистанционными называет преступления, которые совершаются без физического контакта с потерпевшими[3]. На наш взгляд, такое понимание дистанционного мошенничества не отражает всех специфических черт, присущих данным деяниям.

В научных источниках встречаем и такую, в целом удачную, с нашей точки зрения, формулировку дистанционного мошенничества — это мошенничество, «при котором виновный, чаще всего используя компьютерные и телефонные сети, воздействует на сознание потерпевшего путем обмана, склоняет к передаче имущества удаленным образом»[4].

Заслуживает поддержки суждение А.А. Лебедевой, которая полагает, что «в настоящее время в науке сформировалось понятие “дистанционное мошенничество”, включающее в себя: телефонное

---

1 *Ожегов С.И.* Толковый словарь русского языка. URL: https://slovarozhegova.ru/word. php?wordid=6679 (дата обращения: 25.09.2020).

2 Дистанционное управление // Большая российская энциклопедия. URL: https://bigenc.ru/technology_and_technique/text/1959222 (дата обращения: 25.09.2020).

3 Система против системы. Как раскрывают дистанционные преступления // Еженедельник «Аргументы и факты». 2017. № 45. АиФ-Алтай. URL: https://altai.aif.ru/society/sistema_protiv_sistemy_kak_raskryvayt_distancionnye_ prestypleniya (дата обращения: 15.07.2019).

4 *Кудрявцев Р.В.* Организация деятельности по раскрытию дистанционных мошенничеств // Молодой ученый. 2019. № 24 (262). С. 218–221.

мошенничество; мошенничество с использованием сети Интернет; мошенничество с использованием электронных средств платежа (ст. 159.3 УК РФ)»[1]. Однако автор не раскрывает здесь все средства, используемые при совершении преступлений рассматриваемой категории.

Не все средства совершения дистанционного мошенничества выделяют Н.Н. Потапова и О.И. Долгачёва, полагая, что «особую обеспокоенность руководства МВД России вызывают получившие широкое распространение мошенничества, совершаемые с использованием банковских карт, сети Интернет и средств мобильной связи (далее — дистанционные мошенничества)»[2].

Свое видение сути исследуемого понятия изложил М.С. Большаков: «В отечественной следственной практике уже несколько лет активно используется термин “дистанционные мошенничества”, суть которых сводится к совершению хищений чужого имущества путем обмана людей без непосредственного физического контакта с ними с использованием различных средств связи»[3].

Н.Н. Горач предлагает несколько иную трактовку «вида преступлений, которые совершаются с использованием непосредственно средств связи, т.е. дистанционно»: «В нашем случае наиболее актуальны телефонная и сотовая связь, так как больше всего преступлений совершаются именно с помощью них, а именно, мошенничество. Данная новая категория стала именоваться как дистанционное мошенничество с использованием средств проводной и мобильной, телефонной связи»[4]. Представленная формулировка,

---

1 *Лебедева А.А.* Особенности взаимодействия следователя и сотрудников оперативных подразделений при расследовании преступлений в сфере дистанционного мошенничества // Процессуальные и организационно-правовые особенности взаимодействия органов предварительного расследования с органами, осуществляющими оперативно-разыскную деятельность: проблемы и пути их решения: мат-лы междунар. науч.-практич. конф. / под общ. ред. А.М. Багмета. М.: Московская академия СК России, 2018. С. 124.

2 *Потапова Н.Н., Долгачева О.И.* Прогнозирование и планирование в деятельности следователей и оперуполномоченных уголовного розыска при раскрытии и расследовании фактов дистанционных мошенничеств // Вестник Казан. юрид. ин-та МВД России. 2018. № 2 (32). С. 247.

3 *Большаков М.С.* Общие условия расследования дистанционных мошенничеств // Общественная безопасность, законность и правопорядок в III тысячелетии. 2019. № 5-1. С. 277.

4 *Горач Н.Н.* Актуальные вопросы производства предварительного следствия: теория и практика: сборник научных трудов всероссийской научно-практической конференции 11 апреля 2019 г. М.: Московский университет МВД России им. В.Я. Кикотя, 2019. С. 116–117.

на наш взгляд, затрагивает некоторые характерные черты таких преступлений, однако является крайне абстрактной и не содержит в себе конкретики, отображающей специфику дистанционного мошенничества.

Н.Д. Литвинов и А.Н. Федоров верно отмечают, что «появление средств мобильной связи привело к зарождению совершенно нового вида преступления — хищения денежных средств путем дистанционного обмана либо злоупотребления доверием (дистанционного мошенничества)»[1]. Но полного определения ему не дают.

Таким образом, мы наблюдаем в науке и практике самые разные представления о дистанционном мошенничестве. Безусловно, указанное понятие требует дальнейшей проработки, в том числе с учетом интересов оперативно-розыскной теории и практики.

Следуя изложенным выше требованиям к формулированию понятий, представляется важным рассмотреть признаки, которые, с нашей точки зрения, характеризуют дистанционное мошенничество и имеют значение для его выявления и раскрытия оперативно-розыскными средствами и методами. А далее выделим из них те существенные признаки, которые должны войти в определение исследуемого понятия.

Во-первых, уголовное законодательство определяет мошенничество как преступные действия, направленные на хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием. Толкование понятий, раскрывающих суть мошенничества, можно найти в решениях Верховного Суда РФ, в многочисленных комментариях к УК РФ, научной и учебной литературе. Знание оперативными сотрудниками объективной стороны мошенничества крайне необходимо как ориентир в деятельности по поиску и получению доказательственной информации по такой категории дел.

Во-вторых, для дистанционного мошенничества характерно то, что преступник не входит в непосредственный физический контакт с потерпевшим, а устанавливает и поддерживает контакт с ним на расстоянии. При этом преступник выдает себя за кого угодно, дезинформирует, вводит потенциальную жертву в заблуждение и вынуждает добровольно передать ему свою собственность. Данный фактор во многом определяет содержание организации и тактики

[1] *Литвинов Н.Д., Федоров А.Н.* Мошенничество с использованием средств мобильной связи (дистанционное): понятие и особенности совершения // Научно-исследовательские публикации. 2015. № 12. С. 73.

проведения ОРМ по документированию преступных действий, установлению лиц, совершающих дистанционные мошенничества.

В-третьих, одним из существенных признаков дистанционного мошенничества является его совершение с использованием современных информационно-телекоммуникационных технологий, которые включают в себя, если обратиться к решению коллегии МВД России от 1 ноября 2019 г. № 3км, использование банковских карт, информационно-телекоммуникационной сети Интернет, средств мобильной связи и компьютерной техники[1].

Практически аналогичный подход к выделению разновидностей мошенничества, совершаемых с использованием современных информационных технологий, мы наблюдаем и в других ведомственных нормативных актах[2].

Знание «технологии» совершения дистанционного мошенничества обеспечивает целенаправленную работу по поиску информации о следах преступной деятельности, их обнаружению и фиксации оперативно-розыскными средствами и методами.

В-четвертых, для дистанционного мошенничества характерны: высокая степень скрытности преступных действий, наличие возможностей сокрытия преступниками следов преступной деятельности и своего места нахождения. Существенным препятствием для их идентификации является возможность использования ими различных программных технологий, позволяющих, к примеру, менять IP-адрес пользователя в сети Интернет, а также применять технологии «подменных» абонентских номеров посредством SIP-телефонии.

Указанное обстоятельство, характеризующее дистанционное мошенничество, требует поиска новых профессиональных подходов к противодействию указанным преступлениям на основе более тесного межрегионального, межведомственного взаимодействия.

---

[1] Об объявлении решения коллегии Министерства внутренних дел Российской Федерации от 1 ноября 2019 г. № 3км «О мерах по совершенствованию организации работы по выявлению, раскрытию и расследованию преступлений, совершаемых с использованием информационно-коммуникационных технологий»: приказ МВД России от 25 ноября 2019 г. № 878 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=EXP&n=519451#W4WNegSYH3nGzvxY1 (дата обращения: 10.12.2020).

[2] См., например, приказ МВД России от 3 апреля 2018 г. № 196 «О некоторых мерах по совершенствованию организации раскрытия и расследования отдельных видов хищений».

В-пятых, дистанционное мошенничество является преступлением, имеющим зачастую межрегиональный характер. Благодаря техническим средствам и сетям преступник получает доступ к неограниченному количеству объектов своего посягательства, независимо от их территориального местоположения.

Массовость охвата преступниками потенциальных жертв в различных субъектах РФ создает существенные трудности в координации действий оперативно-розыскных, следственных органов по раскрытию и расследованию дистанционного мошенничества.

В-шестых, значительная часть дистанционных мошенничеств совершается организованными группами. Преступления тщательно планируются, проводятся подготовительные действия, распределяются роли, вырабатываются способы противодействия их раскрытию и расследованию.

Полагаем, что рассмотренные признаки дистанционного мошенничества достаточно полно характеризуют его как объект оперативно-розыскного научного и практического интереса. Вместе с тем не все из перечисленных признаков следует отнести к существенным и включить в дефиницию дистанционного мошенничества. С нашей точки зрения, к таковым целесообразно отнести:

- хищение чужого имущества путем обмана или злоупотребления доверием;
- установление и поддержание контакта с потерпевшим на расстоянии;
- совершение преступных действий с использованием современных информационно-телекоммуникационных технологий.

С учетом изложенного предлагаем определить дистанционное мошенничество как оперативно-розыскную категорию следующим образом: это *хищение чужого имущества путем обмана или злоупотребления доверием, совершаемое с использованием информационно-телекоммуникационных технологий, позволяющих устанавливать удаленное соединение и поддерживать устойчивый контакт с потерпевшим на расстоянии.*

Раскрывая значение ввода в научный оборот оперативно-розыскного понятия дистанционного мошенничества, отметим следующее.

Прежде всего, указанное понятие целесообразно использовать при разработке частной методики раскрытия указанных преступлений. Несмотря на большое разнообразие мошеннических действий, совершаемых с использованием сети Интернет, мобильной связи и иных средств коммуникации, они имеют одни и те же характеристики, значимые для разработки единой частной методики

их раскрытия. Например, характеристика личности преступников, способы обмана для установления и поддержания контактов с потерпевшими, вхождения к ним в доверие. Типичной является и следовая картина дистанционного мошенничества. Независимо от способов обмана, закономерности образования следов преступных действий в технологической системе коммуникации преступника и потерпевшего остаются практически едиными.

Дистанционное мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий, является самостоятельной обособленной разновидностью противоправных деяний, которую отличает собственная специфика в способах их подготовки, совершения и сокрытия. Соответственно, перед оперативно-розыскной наукой стоит задача разработки эффективной методики их раскрытия, включающей особенности применения в этих целях оперативно-розыскных средств и методов.

* * *

Важно сказать и то, что введение в оборот и использование в научном обиходе терминов, объединяющих определенные виды или группы преступлений, имеющих общие характеристики, является обычной практикой не только для оперативно-розыскной теории, но и для криминалистики, криминологии. В качестве примера здесь можно привести такие термины: «коррупционные преступления», «заказные убийства», «квартирные кражи», «сексуальные преступления», «бытовые преступления» и др. Дистанционное мошенничество следует поставить в этот же понятийный ряд.

А.С. Овчинский

Цифровые платформы оперативно-розыскной профилактики преступлений

1. Эволюция технологий и профилактика преступлений

Профилактика преступлений — это чрезвычайно емкое понятие. На разных стадиях становления и развития криминологии и социологии, психологии и медицины, биологии и генетики, в разных социальных, экономических, исторических условиях профилактика преступлений как опиралась на научные достижения и результаты определенных исследований, так и отражала общественные ожидания, а главное — наличие или отсутствие политической воли побороть или вообще искоренить преступность в тех или иных ее формах, видах, проявлениях.

Волны информатизации дают импульсы все более масштабным подходам к профилактике преступлений. Развивается предиктивная аналитика, позволяющая делать все более обоснованные прогнозы, а по существу — предсказывать развитие тех или иных криминальных ситуаций. Набирают силу системы фиксации поведенческих реакций, действий и поступков людей, например, в ходе протестных массовых мероприятий, грозящих нарушениями общественной безопасности.

Однако одновременно информационные технологии открывают и новые направления преступности. На правоохранительную деятельность весьма многогранно проецируется двойное назначение технологий как в позитивно-конструктивном приложении, так и в негативно-деструктивном плане, приносящем все большие угрозы безопасности. Технологии повышают эффективность мероприятий, направленных на раскрытие и расследование преступлений, но одновременно расширяют спектр угроз, связанных с их использованием при совершении преступлений. В такой ситуации все большую актуальность приобретают новые подходы к предотвращению преступлений.

Можно опираться на общесоциальную профилактику — создание в обществе условий, препятствующих развитию преступности. Ее уровень можно понижать в русле криминологической профилактики — совершенствования уголовного законодательства,

формирования правосознания. Цифровая трансформация, затрагивающая все стороны жизни, несомненно, актуализирует эти направления профилактики преступлений.

Сегодня же, в условиях стремительных изменений, связанных с повышением технологической оснащенности криминальной среды, а по существу — со все более глубоким погружением в виртуальную реальность, сдерживать рост преступлений, и в первую очередь уже киберпреступлений, необходимо на платформах оперативно-розыскной профилактики, а именно превентивных мер по оперативному предотвращению, предупреждению и пресечению преступлений.

Теоретические основы оперативно-розыскной профилактики были заложены отечественными учеными на заре информатизации правоохранительных органов[1]. В течение нескольких десятилетий в этом направлении был накоплен огромный опыт. По мере эволюции технологий (автоматизации, цифровизации, цифровой трансформации) в оперативно-розыскной профилактике все более значимую роль играло информационно-аналитическое сопровождение мероприятий.

Автоматизация обработки данных в правоохранительной деятельности сопровождалась переводом оперативно-розыскных и криминалистических учетов на электронные носители. Создавались банки данных, базы данных, автоматизированные информационно-поисковые системы (АИПС), аппаратно-программные комплексы (АПК), нацеленные на профилактику, раскрытие и расследование преступлений.

Цифровизация была связана с развитием интернет-технологий. К аналитической разведке (в информационных массивах) добавились компьютерная разведка (в сетях и системах обработки и передачи данных), мультимедийные технологии получения и обработки аудио- и видеофайлов, методы и средства информационно-психологических воздействий. Были сделаны шаги в создании пространства обмена данными, эксплуатировалась единая информационно-телекоммуникационная сеть (ЕИТКС), была поставлена на вооружение информационная система обмена данными (ИСОД). Вслед за высокотехнологичными преступлениями в виртуальное пространство сетевых коммуникаций все глубже стала погружаться оперативно-

[1] *Овчинский С.С.* Оперативно-розыскная информация: монография / под ред. А.С. Овчинского, В.С. Овчинского. 2-е изд., доп. М.: ИНФРА-М, 2017.

розыскная деятельность. Многие мероприятия уже проводятся в сетевом эфире.

Цифровая трансформация правоохранительной сферы — это уже использование больших данных и применение систем искусственного интеллекта, биометрия с возможностями распознавания лиц, речи, психоэмоциональных состояний. Цифровая трансформация — это и возможность тотального контроля перемещений, действий, поступков, поведения, потребностей и желаний людей, это и возможность выявления внешних признаков по генетическим следам. Объединить эти возможности должны цифровые платформы: программные, инфраструктурные, отраслевые.

Одновременно технологии меняли и характер преступности. Автоматизация накопления и обработки данных породила преступления в сфере компьютерной информации. Цифровизация, использование сетевых технологий выдали всплеск высокотехнологичных мошенничеств. На первый план выдвинулись угрозы кибертерроризма, обострились проблемы противодействия экстремизму в информационных сферах.

Цифровая трансформация открывает свой «цифровой ящик Пандоры», порождает новые виды преступлений, использующие электронные данные о людях, об их финансовом положении, собственности, об образе жизни и увлечениях, о здоровье и связях. В криминальной социальной инженерии технологии дипфейков — фальшивых мультимедийных продуктов — изменяют ландшафт и многократно расширяют разнообразие киберугроз[1].

На криминальную арену выходит цифровая организованная преступность. Американские эксперты приводят баснословные цифры, указывающие на миллиардные доходы мировой кибермафии. По мнению экспертов, криминальные коммуникации «темного» интернета и трафик, проходящий через них, многократно превосходят нагрузку общедоступных сетей[2]. Открываются перспективы эффективной фальсификации данных, создания фейковых событий, использования цифровых аватаров, информационных муляжей, фантомов, миражей.

При этом спектр наибольших угроз, которые несут современные информационно-коммуникационные технологии, неуклонно сме-

---

[1] *Ларина Е.В.*, *Овчинский В.С.* Криминальная жизнь дипфейков // Завтра. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfejkov (дата обращения: 20.08.2021).

[2] *Овчинский В.С.*, *Жданов Ю.В.* Кибермафия становится глобальным игроком // Завтра. URL: https://zavtra.ru/blogs/kibermafiya_stanovitsya_global_nim_igrokom (дата обращения: 20.08.2021).

щается в сторону воздействий на сознание людей, сообществ, народов. Мы все чаще становимся свидетелями того, как протестные настроения и выступления в разных странах мира переходят в погромы, открытые грабежи, гражданские конфликты, кровавые столкновения.

В этой ситуации еще острее ощущается необходимость использовать возрастающие возможности современных технологий в профилактических воздействиях на криминальную среду, а в более общем плане — на ту среду, в которой накапливаются потенциалы социальной деструкции, формируются корни терроризма, прорастают споры экстремизма. И здесь наряду с научными проблемами формирования личности преступника (уже в современной цифровой среде) на первый план выступают практические задачи своевременного выявления лиц, от которых можно ожидать асоциального поведения, противоправных действий, совершения преступлений.

2. Возможности выявления потенциальных преступников по цифровым данным

Изучение личности преступника можно рассматривать как одно из ключевых направлений развития криминологии. Более двух столетий обсуждается влияние самых разнообразных факторов на зарождение, формирование и реализацию криминальных наклонностей[1]. В первую очередь это требуется именно для профилактики преступлений, для того, чтобы понять, какие превентивные меры общественного или социального контроля, правового или административного регулирования, оперативно-розыскного противодействия или информационно-психологического противоборства необходимы для предотвращения или пресечения преступной деятельности. Не раз предпринимались попытки спрогнозировать возможное развитие ситуаций, в которых могут накапливаться и реализовываться криминальные потенциалы, а лучше — непосредственно предсказать (с определенной вероятностью) совершение того или иного преступления определенным лицом.

Для создания цифровых платформ оперативно-розыскной профилактики преступлений необходимо в первую очередь иметь алгоритмы выявления лиц, от которых можно ожидать асоциального поведения, правонарушений, преступлений.

Попытки выявления потенциальных преступников предпринимались не раз. На ранних стадиях криминологических иссле-

[1] *Овчинский В.С.* Криминология и биотехнологии. М.: Норма, 2005.

дований пытались связать то или иное преступление с антропологическими признаками человека: узкий лоб, близко посаженные глаза, длинные пальцы... В последующем, оценивая вероятность криминальной активности, исходили из среды воспитания, подозрительных знакомств, погружения в криминальную субкультуру, проявлений лживости, жестокости, неуживчивости, извращенных амбиций...

Сегодня открываются реальные возможности вычислить потенциального преступника на основе анализа всей совокупности цифровых данных, которые можно получить практически о каждом человеке. Системное накопление данных о людях, о жителях стран и регионов осуществляется уже более 20 лет.

В США это делается относительно открыто после известного теракта 11 сентября 2001 г. В результате принятия ряда законов, направленных на борьбу с терроризмом, спецслужбы США стали осуществлять контроль переговоров, сообщений, перемещений, финансовых транзакций. По существу, стали накапливаться данные обо всех лицах, попадающих в поле зрения правоохранительных органов, разведывательных и контрразведывательных служб, т.е. обо всех людях, которые потенциально могли представлять угрозу безопасности.

Заметим, что задолго до этого параллельно с правоохранительными и государственными структурами огромные объемы данных о гражданах, имеющих отношение к тем или иным объединениям (политическим, религиозным, этническим, профессиональным), накапливались в многочисленных так называемых общественных фондах. Разнообразные «фонды» тесно сотрудничали с информационно-аналитическими центрами спецслужб и органов безопасности, а по существу — выполняли их функции еще в доцифровую эпоху.

Из года в год круг контролируемых лиц быстро расширялся. В связи со стремительным развитием электронных коммуникаций, с экспоненциальным увеличением вычислительных мощностей и объемов генерируемых данных не исключено, что на сегодняшний день практически на всех людей, проживающих постоянно или временно в стране, заведены достаточно объемные электронные досье.

Не приходится сомневаться в том, что эти электронные досье «работают», т.е. эффективно используются при решении правоохранительных задач. В хаосе политической борьбы последних лет, протестных выступлений, переходящих в погромы и столкновения с полицией (вплоть до захвата Капитолия в Вашингтоне), американским правоохранительным органам удается устанавливать

и привлекать к ответственности сотни зачинщиков, подстрекателей и активных участников беспорядков.

В целом, в технологически развитых странах мероприятия по обеспечению национальной безопасности и непосредственно противодействие внутренним и внешним криминальным угрозам сегодня опираются на «сплавы» оцифрованных данных обо всем, что можно зафиксировать. Так, уже имеется опыт установления лиц, причастных к террористической деятельности, на основе выявления определенных закономерностей в череде разрозненных событий. Например, если вероятность последовательности ситуаций, связанных с некоторым лицом, оказывается меньше некоторого заданного порога, то это может стать сигналом к проведению розыскных мероприятий и расследований.

В Китае накопление данных о жителях страны происходит подчеркнуто открыто и весьма масштабно в рамках ставшей широко известной системы «социального кредита». Грандиозный социальный эксперимент охватил уже практически все провинции 1,5-миллиардной страны. Для каждого жителя вычисляется его индивидуальный рейтинг, состоящий из положительных баллов за примерное поведение и хорошие поступки и отрицательных баллов за нарушения общественного порядка, проявление неуважения к окружающим, неблаговидные поступки. Такая рейтинговая оценка, а по существу — ранжирование граждан, позволяет включать дополнительные механизмы регулирования общественных отношений, стимулируя людей к «правильному» образу жизни.

Естественно, китайская система кредита получает весьма неоднозначные и, как правило, негативные оценки со стороны мирового либерально ориентированного общественного мнения. При этом китайский эксперимент продолжается, система рейтингов совершенствуется. Искусственные нейросети обрабатывают все большие объемы данных.

Важно отметить, что китайский подход в сборе, накоплении и использовании данных о гражданах своей страны имеет ярко выраженную профилактическую направленность. Преследуется цель искоренить какие-либо противоправные действия не столько за счет выявления и пресечения возможных преступлений, сколько путем прямых, можно сказать, весьма откровенных воспитательных воздействий, включающих как поощрения некими привилегиями, так и наказания путем ограничения или лишения определенных прав.

Сравнивая «западные» и «восточные» подходы к сбору, накоплению и использованию данных для профилактики преступлений,

можно отметить, что Северная Америка и Западная Европа концептуально ближе к криминологической профилактике, опирающейся на угрозы привлечения «профилактируемых» лиц к административной и уголовной ответственности. В то же время в сложившихся китайской, корейской (Южная Корея), сингапурской весьма эффективных системах предупреждения преступлений просматриваются контуры фоновой общесоциальной профилактики. Эта профилактика построена в первую очередь на использовании все более возрастающих возможностей информационно-телекоммуникационных средств и технологий оказывать целенаправленные воспитательные воздействия на сознание жителей своих стран. Такие воздействия, которые учитывают исторические традиции, политические системы, государственные идеологии, мировоззрение и менталитет народов.

В России в последние годы также накапливаются огромные объемы самых разнообразных цифровых данных о людях, об их профессиональных компетенциях и потребностях, об увлечениях и перемещениях, об операциях с финансовыми активами и недвижимостью. Данные собираются, накапливаются и обрабатываются на цифровых платформах крупных предприятий и объединений сферы торговли и услуг. Транспортные базы данных содержат сведения о перемещениях граждан железнодорожным, авиационным, морским транспортом, о междугородных автобусных перевозках. Разнообразные данные накапливаются на серверах и порталах государственных услуг. Они накапливаются в процессе медицинских и антипандемических мероприятий. Медицинские карточки с историями болезней десятков миллионов людей уже представлены в электронном виде.

Возрастают потоки данных, которые фиксируются многочисленными камерами видеонаблюдения. Данные поступают из городских, транспортных, дорожных сетей видеонаблюдения. Все более широкое распространение получают системы биометрии, позволяющие выявлять и отслеживать перемещение и местоположение конкретных людей. Видеонаблюдением и автоматической фиксацией событий оснащены системы охраны самых разнообразных предприятий и учреждений. Накапливаются электронные данные о финансовых операциях как предприятий, так и физических лиц, которые во все больших объемах осуществляют безналичные расчеты.

Обратим внимание на то, что пока речь идет о накоплении огромных объемов данных вне сферы деятельности органов внутренних дел. Но при раскрытии и расследовании преступлений

часто именно использование этих данных играет решающую роль — например, фиксация криминального события видеокамерами или установление места пребывания (маршрутов передвижения) подозреваемых на основе использования транспортных баз данных и т.д.

Таким образом, огромные массивы данных, накапливаемых вне правоохранительной сферы, становятся информационной средой, в которой проводятся ОРМ и следственные действия. Эти данные можно представить некоей фоновой оперативно-розыскной информацией. Естественно, возникают вопросы: насколько правомерно использовать эту фоновую оперативно-розыскную информацию непосредственно для профилактики преступлений и как это делать эффективно?

Одновременно мы обращаемся к ресурсам данных, накапливаемых уже непосредственно специализированными подразделениями правоохранительных органов. В ОВД создана и функционирует своя система получения, накопления и обработки данных о людях, причастных к тем или иным происшествиям, правонарушениям, преступлениям. Эта система имеет вековую историю. Еще в Российской империи осуществлялись весьма обстоятельная регистрация и накопление массивов данных о лицах, как совершивших те или иные преступления, так и подозреваемых в их совершении.

Сегодня на вооружении у правоохранительных органов стоят автоматизированные информационно-поисковые системы и программно-аппаратные комплексы, нацеленные на раскрытие и расследование преступлений. В электронный вид переводятся оперативно-розыскные и криминалистические учеты, данные о людях, совершивших преступления, накапливаются в системе исполнения наказаний.

В органах внутренних дел были созданы и многие годы успешно функционировали специализированные аналитические подразделения — Центры оперативно-розыскной информации. В настоящее время эти подразделения подверглись реформированию. Но именно эти подразделения оснащены автоматизированными информационными системами и аппаратно-программными комплексами, основное назначение которых — информационно-аналитическое сопровождение мероприятий по раскрытию преступлений и обеспечению безопасности. При этом кроме основного назначения эти системы и комплексы формируют непрерывно пополняемые информационные ресурсы. Эти информационные ресурсы могут быть использованы в инициативной или предиктивной оперативно-розыскной аналитике. Они могут составить основу и криминологиче-

ских исследований, направленных на профилактику преступлений, и непосредственно выявления наиболее криминально опасных лиц с предсказанием ожидаемых преступлений. Таким образом, к услугам криминологов уже имеются весьма объемные информационные массивы данных.

3. Многофункциональная цифровая платформа и автоматизация выявления криминально опасных лиц

Целенаправленный сбор данных и составление полномасштабных цифровых «досье» на людей, попадающих в поле зрения правоохранительных органов, требуют определенной нормативно-правовой базы. В этих вопросах сложно ожидать общественного консенсуса. Но проблема назрела. Данные о происшествиях, преступлениях, правонарушениях непрерывным потоком поступают, фиксируются и накапливаются в разных службах органов внутренних дел. Естественно, накапливаются данные и о лицах, причастных к тем или иным инцидентам. В ходе уже раскрытия и расследования преступлений в информационные центры ОВД поступают запросы на предмет установления причастности тех или иных лиц к преступлениям и происшествиям. Эти запросы обрабатываются и также пополняют ресурсы данных о лицах, попадающих в поле зрения ОВД.

Для объединения потоков поступающих разнородных данных, их накопления и возможности использования в криминологических исследованиях, направленных на профилактику преступлений, были разработаны специальные программные сервисы, совокупность которых представляет собой цифровую платформу многофункционального назначения.

Разработка «идеологии» такой цифровой платформы и ее создание были осуществлены сотрудниками Центра оперативно-розыскной информации Главного управления МВД России по Московской области совместно с сотрудниками Учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя.

По специально разработанным алгоритмам выделялись блоки данных, связанных с конкретными лицами, совершившими преступления, нарушителями общественного порядка, наркоманами, злостными пьяницами, подозреваемыми в причастности к определенным преступлениям. Были получены авторские патенты (свидетельства о государственной регистрации программ для ЭВМ)

на 26 сервисов, составивших программную цифровую платформу многофункционального назначения[1].

Основные серверы цифровой платформы «РЕГИСТРАЦИЯ СОБЫТИЙ», «ВЫЯВЛЕНИЕ ПРЕСТУПЛЕНИЙ», «ФИЗИЧЕСКИЕ ЛИЦА», «БИОМЕТРИЧЕСКИЕ ПРИЗНАКИ» позволяют осуществлять:

— формирование поисковых запросов по объектам исследования;
— категоризацию установочных данных по объекту поиска;
— сбор и хранение анкетных данных по объекту исследования;
— проверку лиц по заданным параметрам;
— установление местоположения объекта поиска;
— фиксацию ключевых особенностей — «окраса» преступления;
— выявление признаков серийности;
— выборку и категоризацию отдельных видов преступлений;
— проверку лиц, представляющих оперативный интерес;
— вычленение данных, представляющих оперативный интерес;
— обработку поступающих медиафайлов;
— фотоучет по поступающим данным;
— формирование ресурсов данных об изъятых и запрещенных предметах;
— формирование статистических данных.

Цифровая платформа включает серверы «СИНХРОНИЗАЦИЯ ДАННЫХ» и «КОНВЕРТАЦИЯ ДАННЫХ», серверы «ФОРМИРОВАНИЕ ДОКУМЕНТОВ» и «ИНДЕКСАЦИЯ ДОКУМЕНТОВ», сервер «КОНТРОЛЬ ОПЕРАТОРОВ».

На базе цифровой платформы проведено исследование возможности выявления лиц, представляющих угрозы антикриминальной безопасности. Это исследование опиралось на фундаментальное достижение криминологической мысли, а именно на утверждение о том, что «***накопление отклонений от позитивного поведения может приводить человека к преступлению***». Заметим, что это «утверждение» было проверено еще в прошлом веке в ходе апробации самых первых автоматизированных информационно-поисковых систем оперативно-розыскного назначения.

---

[1] Свидетельства о государственной регистрации программ для ЭВМ (авторы: Б.Р. Аветисян, К.Р. Аветисян, В.Э. Боль, К.К. Борзунов, А.Б. Ерохин, А.С. Овчинский). Правообладатель — Федеральное государственное казенное образовательное учреждение высшего образования «Московский университет МВД России имени В.Я. Кикотя». 2020.

При создании и апробации информационно-поисковых систем в нашей стране в 70-е гг. прошлого века были предприняты попытки на основе поступающих и фиксируемых (а точнее кодируемых на перфокартах) сообщений выявить наиболее криминально опасных лиц.

В настоящее время для понимания сути проблемы весьма важным представляется качественный анализ содержания информационных сообщений, которые составляли оперативно-розыскные ресурсы данных, используемых более полувека назад для раскрытия и профилактики преступлений[1].

В одной из весьма представительных совокупностей сообщений о лицах, которые привлекали внимание правоохранительных органов: 32% оказались участниками групп с антиобщественной ориентацией; 33,7% допускали систематические посягательства на граждан в форме оскорбления, унижения их чести и достоинства; 31,5% совершали мелкие хищения; 15% предоставляли свои квартиры для сборищ на почве пьянства и разврата; 3,2% изготовляли ножи и другое оружие; 12,1% были замечены в попытках вовлечения несовершеннолетних в преступную деятельность; 5,6% домогались половой близости в циничной форме; 2% употребляли наркотики.

Обратим внимание и на то, что в практике формирования информационных массивов первых автоматизированных систем обработки данных был опыт отражения нравственных характеристик выявленных лиц: 50,8% допускали грубое обращение с людьми, проявляли злобность и агрессию; 46,6% проявляли лживость и склонность к обману; 33,2% — крайний эгоизм и пренебрежительное отношение к законам; 10% — циничное отношение к женщине; 30% состояли на учете в лечебных учреждениях в связи с алкоголизмом и отклонениями в психике.

Таким образом, еще задолго до «цифровой эпохи» информационно-поисковые системы открывали перед криминологами перспективы создания и исследования ***«криминальных профилей»***. Речь идет о таких «криминальных профилях», которые сегодня можно получать, используя самообучающиеся нейронные сети в обработке больших данных, генерируемых и накапливаемых социальными сетями.

---

[1] *Овчинский С.С.* Оперативно-розыскная информация: монография / под ред. А.С. Овчинского, В.С. Овчинского. 2-е изд., доп. М.: ИНФРА-М, 2017.

Практически же в прошлом веке выявление наиболее криминально активных личностей осуществлялось информационно-поисковой подсистемой «СИГНАЛ» путем суперпозиции массивов данных о лицах, обладающих тем или иным негативным признаком. Посредством последовательной фокусировки, можно сказать, математических процедур, характерных для теории множеств или булевой алгебры, выявлялись группы лиц, обладающих наибольшей совокупностью таких качеств и требующих незамедлительных профилактических воздействий и проверки причастности к уже совершенным преступлениям.

Результаты были уже в ходе экспериментальной апробации информационно-поисковых систем. Так, работники уголовного розыска одного из городских отделов внутренних дел, «фокусируя» накопленные данные, в течение 1974 г. раскрыли 18 тяжких преступлений: грабежей, краж, телесных повреждений.

Создатели первых автоматизированных информационно-поисковых систем и программных комплексов для электронно-вычислительных машин вместе с разработчиками теории оперативно-розыскной аналитики неоднократно отмечали, что «***для надежности прогностических выводов необходима временная привязка информации к конкретному моменту или интервалу времени». Указывалось также на «необходимость привлечения дополнительной информации, которая координирована во времени с изучаемым явлением***». И более того, утверждалось, что «***коль скоро мы имеем дело с процессами "накопительного характера", желательна непрерывная регистрация происходящих событий***»[1]. В наше время это стало реальностью.

4. Формирование массива данных для предсказания преступления

Как уже отмечалось, непрерывная регистрация происходящих событий сегодня осуществляется автоматизированными информационными системами, которые фиксируют, накапливают и обрабатывают данные о лицах, попадающих в поле зрения правоохранительных органов. Речь идет о нарушителях общественного порядка, злостных пьяницах, наркоманах, хулиганах, причастных к распространению наркотиков, кражам, ограблениям, разбоям, другим самым разнообразным правонарушениям и преступлениям. Кроме

[1] *Овчинский А.С.* Оперативно-разыскная аналитика (ответ современным угрозам). М.: Издательский дом И.И. Шумиловой, 2015.

того, речь идет о лицах, проверяемых на причастность к преступлениям и происшествиям.

Перед криминологией цифрового мира открывается задача оценить вероятность преступления, которое может быть совершено тем или иным человеком. Как уже отмечалось, задача эта может быть решена не на основе изучения физиологических или психологических особенностей, врожденных или приобретенных комплексов и не на основе анализа социальных условий и неудовлетворенных потребностей и амбиций (хотя информация и об этом будет полезна и может использоваться по мере расширения возможностей систем искусственного интеллекта в распознавании и привлечении необходимых данных из сетевого эфира), а на основе накопления «отклонений от позитивного» поведения и на основе накопления данных о возможной причастности объекта исследования к расследуемым преступлениям.

В процессе исследования использовались результаты автоматической обработки данных на многофункциональной цифровой платформе. По специально разработанным алгоритмам выделялись блоки данных, связанных с конкретными лицами, совершившими преступления, нарушителями общественного порядка, наркоманами, злостными пьяницами, подозреваемыми в причастности к определенным преступлениям.

Важно отметить, что все фиксируемые события были строго распределены по времени (число, месяц, год). Для сохранения конфиденциальности данные о фигурантах в криминологических исследованиях были обезличены. Криминальные ситуации были объединены той или иной «окраской».

В результате максимально формализованная информация о каждом из нескольких тысяч фигурантов состояла из порядкового номера и двух столбцов данных: время события (число, месяц, год) и окраска соответствующего события (см. табл. 1 соответственно на лиц № 160971, 161632, 314291, 629714).

Окраска различных событий и ситуаций, предложенная сотрудниками ЦОРИ ГУВД по Московской области, включала такие основные позиции, как ВОР; НАРКОМАН; ГРАБИТЕЛЬ; АДМИНИСТРАТИВНОЕ ПРАВОНАРУШЕНИЕ; ПЬЯНИЦА; НАСИЛЬНИК; РАЗБОЙНИК; УГРОЗА УБИЙСТВОМ; НЕЗАКОННЫЙ ОБОРОТ НАРКОТИЧЕСКИХ СРЕДСТВ; ХУЛИГАН; ПОДОЗРЕВАЕМЫЙ.

Таблица 1

Данные на подучетных лиц

Данные на лицо № 160971	
Дата события	Окраска события
16.04.2010	ГРАБИТЕЛЬ
16.04.2010	ВОР
16.04.2010	ГРАБИТЕЛЬ
16.04.2010	ВОР
25.05.2010	ГРАБИТЕЛЬ
25.05.2010	ГРАБИТЕЛЬ
04.08.2010	ГРАБИТЕЛЬ
04.08.2010	ГРАБИТЕЛЬ
09.08.2010	ГРАБИТЕЛЬ
09.08.2010	ГРАБИТЕЛЬ
29.05.2013	ВОР
29.05.2013	ВОР
26.09.2015	ВОР
26.09.2015	ВОР
14.10.2015	НЕЗАК. ОБОРОТ НАРКОТ.
14.10.2015	НЕЗАК. ОБОРОТ НАРКОТ.
02.02.2016	НЕЗАК. ОБОРОТ НАРКОТ.
02.02.2016	НЕЗАК. ОБОРОТ НАРКОТ.
24.03.2016	НЕЗАК. ОБОРОТ НАРКОТ.
24.03.2016	НЕЗАК. ОБОРОТ НАРКОТ.
02.06.2016	ВОР
02.06.2016	ВОР
02.06.2016	ВОР
02.06.2016	ВОР

Данные на лицо № 314291	
Дата события	Окраска события
07.07.2010	ВОР
16.01.2014	ВОР
05.03.2014	ПОДОЗРЕ-ВАЕМЫЙ
21.04.2014	АДМ. ПРАВОНА-РУШЕНИЕ
12.05.2014	ВОР
12.05.2014	ВОР
23.07.2014	ГАСТАРБАЙТЕР
13.10.2014	НАРКОМАН
23.10.2014	НАРКОМАН
05.06.2015	ПЬЯНИЦА
05.06.2015	ПЬЯНИЦА
13.07.2015	НАРКОМАН
18.07.2015	ПЬЯНИЦА
22.08.2015	ПЬЯНИЦА
27.08.2015	НАРКОМАН
11.01.2016	ВОР
11.01.2016	ВОР
15.01.2016	ВОР
14.02.2016	ГАСТАРБАЙТЕР
18.04.2016	ГРАБИТЕЛЬ
19.04.2016	ВОР
19.04.2016	ВОР
22.04.2016	ГАСТАРБАЙТЕР
27.05.2016	АДМ. ПРАВОНА-РУШЕНИЕ
22.06.2016	НАРКОМАН
06.01.2017	НАРКОМАН

Окончание табл. 1

Данные на лицо № 161632	
Дата события	Окраска события
14.06.2013	ПОДОЗРЕВАЕМЫЙ
14.06.2013	ПОДОЗРЕВАЕМЫЙ
16.10.2014	НАРКОМАН
16.10.2014	НАРКОМАН
17.12.2014	ВОР
17.12.2014	ВОР
13.02.2016	АДМ. ПРАВОНАРУШЕНИЕ
13.02.2016	АДМ. ПРАВОНАРУШЕНИЕ
09.03.2016	ПЬЯНИЦА
09.03.2016	ПЬЯНИЦА
22.07.2016	ВОР
22.07.2016	ВОР
07.09.2016	АДМ. ПРАВОНАРУШЕНИЕ
07.09.2016	АДМ. ПРАВОНАРУШЕНИЕ
28.07.2017	ГРАБИТЕЛЬ
28.07.2017	ГРАБИТЕЛЬ
12.01.2018	ВОР

Данные на лицо № 629714	
Дата события	Окраска события
03.05.2010	ГРАБИТЕЛЬ
21.06.2010	УГОНЩИК
14.05.2012	НАРКОМАН
14.05.2012	ГРАБИТЕЛЬ
14.05.2012	УГОНЩИК
14.05.2012	НАРКОМАН
14.05.2012	ГРАБИТЕЛЬ
14.05.2012	ВОР
30.11.2012	ВОР
21.03.2013	ВОР
10.10.2013	ВОР
25.11.2015	БОМЖ
25.11.2015	НАРКОМАН
25.11.2015	ВОР
25.11.2015	ВОР
11.03.2016	НЕЗАК. ОБОРОТ НАРКОТ.
12.03.2016	НАРКОМАН
13.04.2016	АДМ. ПРАВОНАРУШЕНИЕ
28.04.2016	АДМ. ПРАВОНАРУШЕНИЕ
22.08.2016	НЕЗАК. ОБОРОТ НАРКОТ.
22.08.2016	НАРКОМАН

5. Вероятностная модель оценки криминального потенциала личности

Рабочая гипотеза, принятая при построении модели оценки криминального потенциала личности, состояла в предположении, что, попав в поле зрения правоохранительных органов в связи с правонарушениями, пьянством, употреблением наркотиков, возможной

причастностью к совершенным преступлениям или вообще к какому-либо криминальному событию, человек впоследствии, хотя и с весьма малой вероятностью, может совершить преступление.

При этом основная идея возможности предсказания преступления заключается в том, что если с течением времени информация о данном лице оказывается не раз и не два в базе данных криминальных событий, то вероятность того, что непосредственно от этого лица можно ожидать совершения преступления, возрастает[1].

Вычисление вероятности преступления осуществляется на основе известных процедур теории вероятности, применяемых для решения широкого круга задач. Так, исходя из значения вероятности наступления событий при единичном испытании, можно определить его вероятность при нескольких попытках[2].

Например, если известно, с какой вероятностью единичным выстрелом из винтовки может быть сбит пикирующий самолет, то путем определенных расчетов находим вероятность того, что самолет будет сбит, если по нему произведено, скажем, 50, 100 или 200 выстрелов.

В нашем случае принимается, что если фигурант зафиксирован в базе данных происшествий с определенной криминальной окраской, то вводится некое значение вероятности R_i того, что он может совершить преступление. Числовое значение R_i находится в интервале от 0 до 1 (0 — невозможное событие, 1 — достоверное событие).

Числовое значение может зависеть от окраски события, которая отражается индексом i. Как правило, величина R_i не превышает 0,05, т.е. вероятность преступления, совершенного человеком, который единожды попал в поле зрения правоохранительных органов, не превышает 5%. Примечательно, что числовые значения параметра R_i могут уточняться и корректироваться в ходе адаптации построенной модели к реальным данным.

В целом задача сводится к определению вероятности совершения ожидаемого преступления лицом, которое не раз попадало в поле зрения правоохранительных органов, исходя из некоторого набора значений R_i.

---

[1] *Овчинский С.С.* Преступное насилие. Преступность в городах. М.: ИНФРА-М, 2007.

[2] *Гутер Р.С., Овчинский Б.В.* Основы теории вероятностей. М.: Просвещение, 1967.

На первом шаге решения задачи определяется вероятность того, что при поступлении некоторого «настораживающего» сообщения никакого криминального события в итоге не произойдет. Это значение составит $(1 - R_i)$. Принципиальным моментом является то, что такие ситуации, когда фиксация правонарушения или антиобщественного проступка ни к чему не приводит впоследствии, с позиции классической теории вероятности могут рассматриваться как независимые друг от друга события.

К независимым случайным событиям применима теорема умножения, согласно которой вероятность составного (итогового) события равна произведению вероятностей событий, его составляющих. Таким образом, вероятность того, что преступление не будет совершено, несмотря на накопление сообщений о правонарушениях, вычисляется как произведение вероятностей всех *i*-х событий: $\Pi (1 - R_i)$.

Заметим, что, поскольку значения вероятностей лежат в интервале от 0 до 1, произведение вероятностей независимых событий (чисел менее 1) приводит к уменьшению вероятности итогового события. В нашем случае по мере накопления «тревожных» сообщений вероятность несовершения преступления исследуемым лицом уменьшается. Тогда вероятность противоположного события, а именно ожидаемого преступления, возрастает, и его значение P вычисляется по формуле

$$P = 1 - \Pi (1 - R_i). \quad (1)$$

Расчетное значение вероятности P ожидаемого преступления (его совершения) можно рассматривать как некий коэффициент или параметр криминальности, который может быть использован, например, при выявлении лиц, причастных к расследуемым преступлениям или требующих определенных профилактических мер, или лиц, присутствие которых на том или ином крупном массовом мероприятии недопустимо.

Использование коэффициентов криминальности может быть весьма эффективным при ранжировании лиц, состоящих на профилактических учетах, и в целом, при выявлении наиболее криминально опасных и деструктивно ориентированных личностей.

6. Предиктивные значения параметра криминальности

Значения параметра криминальности, согласно построенной вероятностной модели, возрастают по мере увеличения зафиксиро-

ванных эпизодов, свидетельствующих о возможной причастности исследуемого лица к тем или иным преступлениям. В пределе, при накоплении большого количества эпизодов с различной «окраской», параметр криминальности стремится к единице.

Значение параметра, стремящееся к единице, означает достоверное событие, т.е. в нашем случае, уголовное преступление, совершенное исследуемым лицом.

Естественно, возникает вопрос: какой уровень параметра криминальности можно считать предиктивно значимым, т.е. начиная с какого значения P необходимо оперативно реагировать, например применять меры общесоциальной или оперативно-розыскной профилактики для предотвращения или пресечения возможного преступления?

Для ответа на этот вопрос исследовались массивы данных более чем на тысячу лиц. При этом выделялись две категории лиц, а именно: те, для которых накопление правонарушений и подозрений в причастности к преступлениям не заканчивалось привлечением к уголовной ответственности, и те, на которых были заведены дела по определенным статьям УК РФ.

В первом приближении статистический анализ дал обескураживающий результат. Оказалось, что, ориентируясь лишь на расчетные значения параметра криминальности, вообще не удается разделить лиц, совершивших и не совершивших преступления, а точнее, привлекаемых к ответственности и не привлекаемых по статьям УК РФ.

Однако более детальное исследование, проведенное на весьма объемных массивах данных, выявило весьма показательные закономерности. В результате вычисления параметров криминальности и сопоставления количества лиц, обладающих одинаковыми значениями этих параметров в одной и другой исследуемой категории, было выявлено, например, что среди тех, кто имел значение параметра криминальности $P < 0{,}2$, только 3% совершили преступление, а среди тех, у кого значение этого параметра достигало $P = 0{,}7$, таковых оказалось уже более 20% (табл. 2).

Весьма показательной при этом представляется построенная по данным табл. 2 кривая зависимости относительного количества лиц, совершивших преступление, от значения параметра криминальности P, вычисленного согласно принятой модели (1) (рис. 1).

Таблица 2

Значение параметра криминальности	Относительное кол-во лиц, совершивших преступление, в %	Кол-во лиц «со статьей»	Относительное кол-во лиц, не совершивших преступление, в %	Кол-во лиц «без статьи»	Общее кол-во исследуемых лиц
<0,1	0,12	1	2,17	18	830
<0,2	5,66	47	20,00	186	830
<0,3	7,83	65	44,94	373	830
<0,4	14,46	120	64,82	538	830
<0,5	17,59	146	73,61	611	830
<0,6	19,64	163	76,87	638	830
<0,7	20,24	168	77,71	645	830
<0,8	20,48	170	78,43	651	830
<0,9	20,72	172	78,80	654	830

Рис. 1. Зависимость относительного количества лиц, совершивших преступление, от величины параметра криминальности

Выяснилось, что при увеличении параметра криминальности до 0,6 относительное количество лиц, совершивших преступления, возрастает, но при последующем его увеличении изменяется уже незначительно.

Таким образом, при планировании профилактических мероприятий и при оценке криминальных угроз можно ориентироваться на значения P = 0,6 и выше.

Анализируя построенную зависимость (рис. 1), можно весьма условно выделить определенные интервалы возрастания параметра криминальности P, в которых проявляется (P < 0,2), формируется (0,2 < P < 0,4), накапливается (0,4 < P < 0,6) и реализуется (P > 0,6) криминальный потенциал личности.

Необходимо, однако, учитывать, что полученные числовые значения имеют условный характер. При необходимости они могут быть скорректированы, например, варьированием значений параметров R_i в ходе адаптации построенной модели с учетом поступающих новых данных.

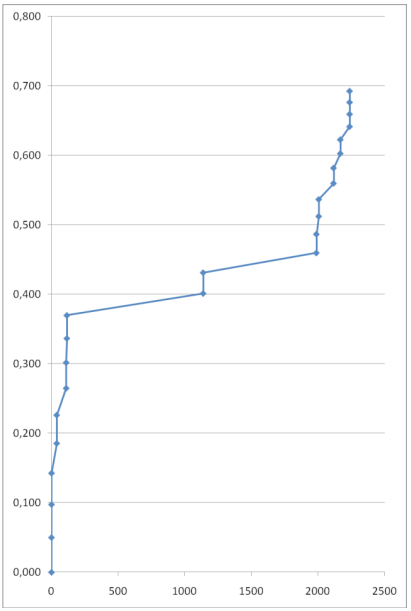
В целом, на этом этапе исследований можно утверждать, что использование расчетных значений параметра P, полученных на основе анализа реально фиксируемых и накапливаемых в информационных системах ОВД данных, дает возможность повысить эффективность выявления криминально опасных лиц, требующих профилактических воздействий и проверки на причастность к совершенным преступлениям.

7. Функции накопления криминальных потенциалов

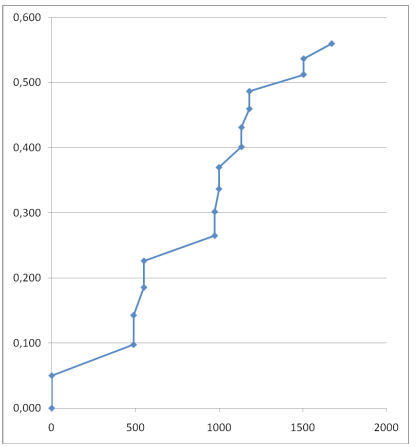
В процессе расчета параметра криминальности формируется цифровой профиль личности с окраской криминальных ситуаций, привязанных к определенным датам (число, месяц, год). Однако для углубленного криминологического анализа социальной, моральной, психологической трансформации личности потенциального преступника наиболее информативным представляется построение функции «накопления личностных повреждений» или функции «накопления криминальных потенциалов».

Эта функция также строится на основании выражения (1). Но в отличие от классической экспоненты, плавно и неуклонно стремящейся к единице, в нашем случае функция накопления криминальных потенциалов может принимать самый разнообразный вид, поскольку изменения как аргументов (R_i), так и значений функции P связаны со временем (t):

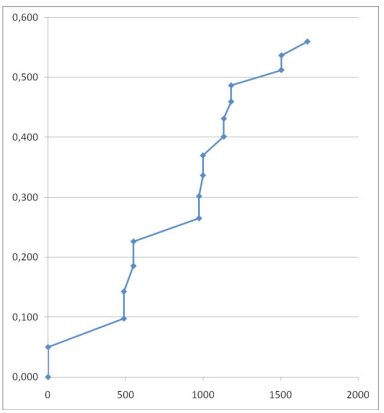
$$P(t) = 1 - \Pi [1 - R_i(t)]. \qquad (2)$$



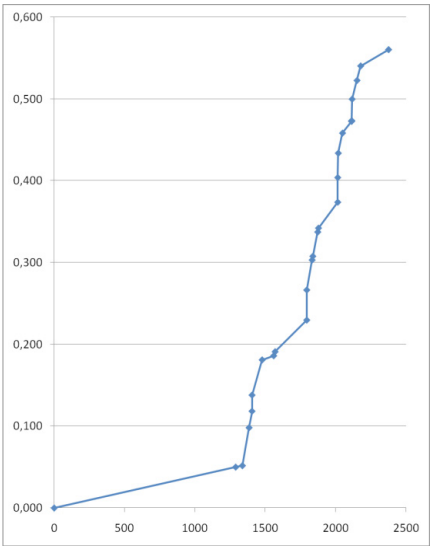
а



б



в



г

Рис. 2. Функция накопления «криминальных потенциалов» во времени (по дням с момента первого появления данных) для лиц:

а — 160971; *б* — 161632; *в* — 314291; *г* — 629714

Проведение анализа того, насколько плавно или резко, скачками или периодами накапливаются «личностные повреждения» или потенциалы деструктивной социально-психологической энергии у того или иного лица, попадающего в поле зрения правоохранительных органов, открывает новые возможности, можно сказать, уже перед оперативно-розыскной криминологией (рис. 2, *а*, *б*, *в*, *г*).

В перспективе на функции «накопления личностных повреждений» или функции «накопления криминальных потенциалов» может опираться инициативная аналитика, например, в обеспечении безопасности массовых мероприятий. Они могут стать базой и для развития предиктивной аналитики, привлекающей к предсказанию преступлений большие данные и использующей системы искусственного интеллекта[1]. При этом основной задачей предиктивной или, можно сказать, оперативной криминологии остается профилактика преступлений.

8. Кодирование криминальной активности

Данные о противоправном поведении, деструктивной деятельности, возможной причастности к совершенным преступлениям, которые в автоматическом режиме накапливаются на десятки и сотни тысяч лиц, открывают перспективы применения систем ИИ как в углублении криминологических исследований, так и в решении практических задач по раскрытию и профилактике преступлений.

Речь может идти об использовании искусственных самообучающихся нейронных сетей для выявления новых тенденций в развитии преступности и автоматизации принятия решений, направленных на обеспечение антикриминальной безопасности на основе распознавания индивидуальных криминальных образов и сопоставления их с обобщенными цифровыми образами разнообразных преступлений.

Опираясь на уже имеющиеся массивы данных, такие цифровые образы нарастания криминальной активности можно получить, если ***наряду с количеством зафиксированных эпизодов оцифровать варианты окраски и последовательности временных интервалов наступления событий, которые с определенной вероятностью приводят человека к преступлению***.

Практически каждой окраске события присваивался двухзначный код (например, ПЬЯНИЦА — 01, НАРКОМАН — 02, АД-

[1] *Овчинский А.С., Борзунов К.К., Чеботарева С.О.* Информационные координаты. Управление. Противоборство. Безопасность. М.: Горячая линия — Телеком, 2018.

МИНИСТРАТИВНОЕ ПРАВОНАРУШЕНИЕ — 03, и т.д.). Весь временной период нарастания криминальной активности делится на кварталы (по три месяца), также с присвоением двухзначного кода (первый квартал — 01, второй — 02, третий — 03, четвертый — 04). Двузначным кодом фиксировалось и непосредственно количество правонарушений (той или иной окраски в том или ином квартале).

Визуально-условный штрих-код нарастания криминальной активности или накопления криминальных потенциалов можно представить в виде штриховых полосок (каждая полоска — зашифрованное событие), расположенных в ячейках таблицы, полученной из оцифрованных окрасок и последовательности временных интервалов (рис. 3–6).

ЛИЦО № 160971

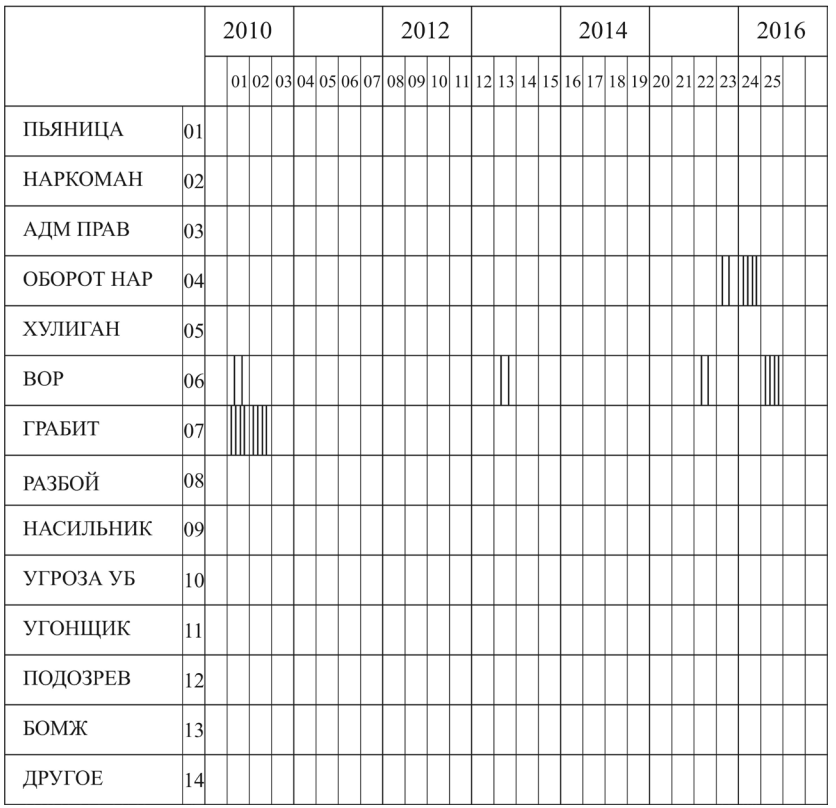


Рис. 3. Визуально-условный штрих-код лица № 160971

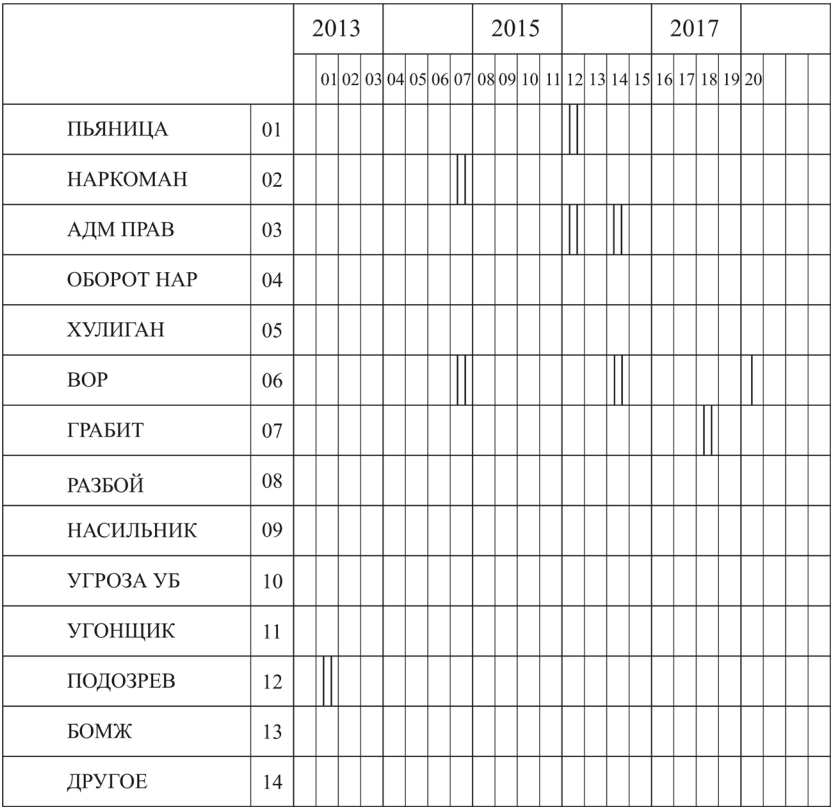


Рис. 4. Визуально-условный штрих-код лица № 161632

Заметим, что считывание информации с подобных таблиц в настоящее время не представляет трудностей для автоматизированных систем, обладающих элементарными функциями распознавания образов.

Однако задачу для искусственного интеллекта можно еще больше упростить, представив криминальные коды исследуемых лиц в виде столбцов чисел, строки которых содержат закодированные данные о том, в каком квартале, какой окраски и сколько событий было зафиксировано (в каждой строке шесть цифр — по три двузначных числа, через пробелы в формате: квартал_окраска_колво) (рис. 7).

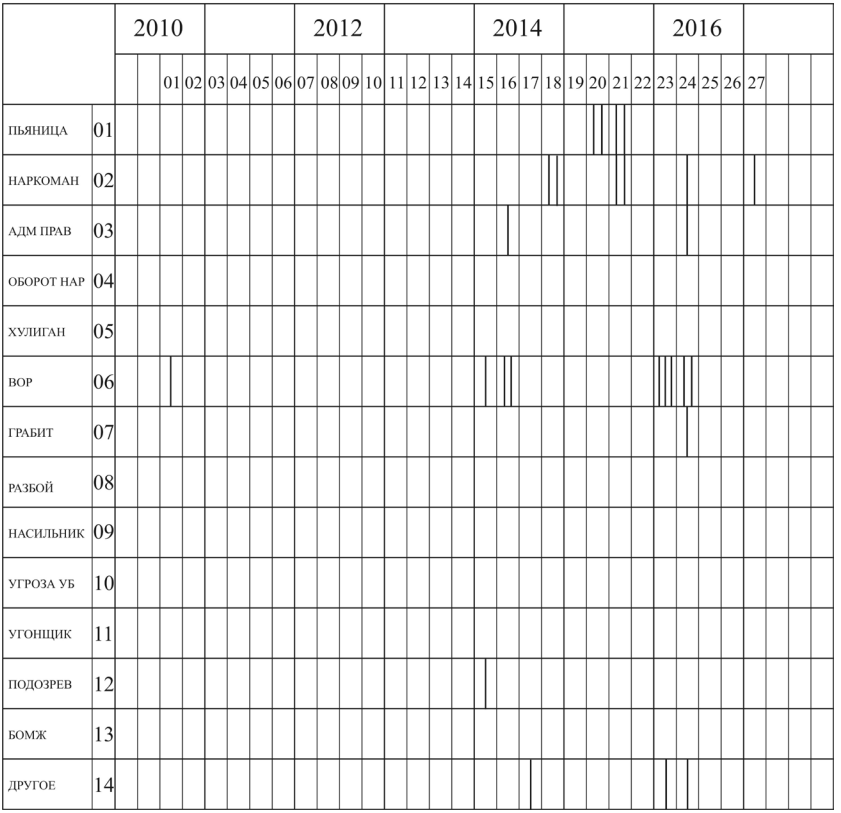


Рис. 5. Визуально-условный штрих-код лица № 314291

В тех случаях, когда нарастание криминальной активности заканчивается преступлением, мы получаем цифровой образ, штрих-код или, можно сказать, индивидуальный криминальный код лица, совершившего определенное преступление.

И здесь отработка искусственным интеллектом больших массивов данных дает возможность на основании известных криминальных кодов получать уже обобщенные криминальные коды для цифровой идентификации различных преступлений.

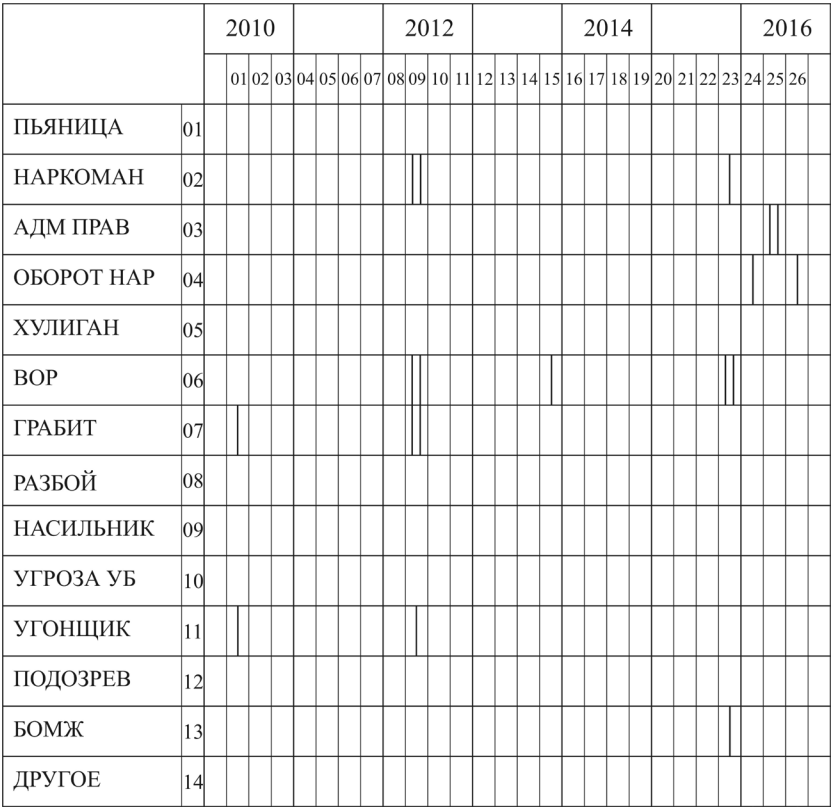


Рис. 6. Визуально-условный штрих-код лица № 629714

Таким образом, использование самообучающихся искусственных нейронных сетей позволит предсказывать вероятность совершения конкретным лицом определенного преступления. Технологически такое предсказание будет осуществляться на основе сопоставления индивидуальных криминальных кодов лиц, попадающих в поле зрения правоохранительных органов, и обобщенных цифровых кодов преступлений, определенных УК РФ.

ЛИЦО № 160971	ЛИЦО № 161632	ЛИЦО № 314291	ЛИЦО № 629714
КРИМ-КОД	КРИМ-КОД	КРИМ-КОД	КРИМ-КОД
01_06_02 01_07_04 02_07_04 13_06_02 22_06_02 23_04_02 24_04_04 25_06_04	01_12_02 07_02_02 07_06_02 12_01_02 12_03_02 14_03_02 14_06_02 18_07_02 20_06_01	01_06_01 15_06_01 15_12_01 16_03_01 16_06_02 17_14_01 18_02_02 20_01_02 21_01_02 21_02_02 23_06_03 23_14_01 24_02_01 24_03_01 24_06_02 24_07_01 24_14_01 27_02_01	01_07_01 01_11_01 09_02_02 09_06_02 09_07_02 09_11_01 12_06_01 15_06_01 23_02_01 23_06_02 23_13_01 24_02_01 24_04_01 25_03_02 26_02_01 26_04_01
а)	б)	в)	г)

Рис. 7. Криминальные коды исследуемых лиц

9. Расширение диапазона используемых данных и повышение эффективности оперативно-розыскной аналитики

В предпринятых исследованиях были использованы пока только реактивные данные, а именно те, которые фиксировались по мере реализации событий или возникновения ситуаций. Заметим, что собственно информация в ее функциональном значении возникает в процессе реакций на внешние воздействия и внутренние побуждения. Реактивные данные при этом формируются по мере поступления сообщений, которые также являются реакцией на происходящее в реальном мире, в виртуальном сетевом пространстве, а может быть, и вообще в воображении человека или массовом сознании.

Другое сущностное проявление информации — ресурсность — обусловлено возможностью фиксироваться, накапливаться и транслироваться на определенных носителях, как естественных — природных, так и искусственных — созданных человеком. Именно

накопленные ресурсы оперативно-розыскных данных, как и ресурсы криминалистической информации, как правило, наиболее востребованы при раскрытии и расследовании преступлений. В перспективе именно эти, годами и десятилетиями формируемые информационные ресурсы правоохранительных органов, должны стать базовыми при получении как индивидуальных цифровых кодов, отражающих уровень и направленность криминальной активности отдельных лиц, так и кодов конкретных преступлений, совершаемых с использованием оружия, взрывных и отравляющих веществ, автотранспортных средств, роботизированных систем.

Наконец, третье фундаментальное проявление информации — фоновое. Оно заключается в отражении окружающей реальности и позволяет рассматривать информацию как атрибут мироздания, наряду с материей и энергией. Развитие представлений о фоновой оперативно-розыскной информации как больших данных, циркулирующих в сетевом эфире и составляющих виртуальную среду ОРД, в настоящее время составляет одно из наиболее перспективных направлений развития как теории, так и практики информационно-аналитического обеспечения правоохранительной деятельности.

Неуклонное внедрение цифровых технологий, стирающих грани между реальным и виртуальным мирами, порождает, можно сказать, и фоновую криминологически значимую информацию. По мере развития и совершенствования систем ИИ будут осуществляться поиск, распознавание и извлечение из интернет-пространства криминологически значимых данных о личности потенциального преступника. Эти фоновые криминологические данные будут обогащать модели и повышать эффективность алгоритмов предсказания преступлений, построенных, в частности, на предлагаемом цифровом кодировании накопления личностных криминальных потенциалов.

Анализируя наиболее перспективные направления оперативно-розыскной аналитики, можно утверждать, что одним из основных программных инструментов, повышающих эффективность решения задач по обеспечению антикриминальной безопасности, могут быть алгоритмы предсказания преступлений.

Экспресс-аналитика в раскрытии преступлений «по горячим следам», как правило, опирается на реактивные данные с места преступления, зафиксированные системой видеонаблюдения. Для установления лиц, причастных к преступлению, используются информационные ресурсы правоохранительных органов, в первую очередь ресурсы оперативно-розыскной информации. При необходимости могут включаться алгоритмы работы с фоновой инфор-

мацией, т.е. поиска данных о подозреваемых лицах в интернете. Эффективность раскрытия преступления с помощью компьютера может быть повышена за счет применения алгоритмов выявления лиц с таким индивидуальным криминологическим кодом, который с наибольшей вероятностью соответствует цифровому коду расследуемого преступления.

Инициативная аналитика при обеспечении безопасности крупнейших массовых мероприятий (Олимпийских игр, Универсиад, Спартакиад, Чемпионатов мира и т.д.) предполагает предварительное исследование всего контингента лиц, участвующих в мероприятии и находящихся на территории его проведения. При этом также используются ресурсы данных о преступлениях, правонарушениях, неуправляемых фанатах и др., которые накоплены как отечественными, так и зарубежными правоохранительными органами и спецслужбами. Применение систем искусственного интеллекта все в большей мере позволяет извлекать и фоновую криминологически значимую информацию из интернета. Лица, представляющие потенциальную угрозу общественному порядку, выявляются и в ходе самих мероприятий, например, стационарными, мобильными или специально оборудованными средствами видеонаблюдения и портретной идентификации. В этом же случае получение, накопление и использование данных об индивидуальных криминологических кодах, т.е. о вероятном совершении определенных преступлений лицами, выявленными в ходе подготовки или проведения мероприятий, поможет оптимизировать оперативные меры по нейтрализации криминальных угроз.

Актуальная аналитика в предсказании «ожидаемого» преступления определенной окраски (грабеж, разбой, изнасилование, квартирная кража и т.д.), с ориентировкой на определенное время и место, а также с выявлением характерных качеств и криминального «почерка» преступников, опирается на алгоритмы анализа криминальной ситуации на обслуживаемой территории (городского района, поселка, региона и т.д.).

В полицейской практике западных стран (США, Канады, Великобритании) оперативные криминологи-аналитики разрабатывают и уже многие годы успешно применяют компьютерные модели и алгоритмы прогнозирования непосредственно преступлений, опираясь на разнообразные данные, накопленные за предшествующие периоды времени. На основании алгоритмов такой актуальной оперативно-розыскной аналитики разрабатываются маршруты патрулирования, организуются засады для пресечения

преступных посягательств, «ловушки» для задержания преступников в определенных местах с учетом рассчитанных интервалов времени ожидания преступления.

Разработка алгоритмов получения данных о конкретных лицах, потенциально «созревших» для совершения преступлений, естественным образом вписывается в комплекс задач, решаемых в рамках актуальной аналитики.

Предиктивная аналитика в настоящее время выходит на первый план в самых разнообразных сферах бизнеса и в первую очередь в маркетинге. Она опирается на революционные прорывы в технологиях накопления, обработки и использования огромных массивов разнообразных данных. При этом содержательное накопление больших данных во многом определяется как запросами потребителей товаров и услуг, так и разнообразными сведениями о самих потребителях, а по существу — обо всех экономически активных гражданах. Крупные торговые сетевые структуры сейчас стремятся узнать «все» о своих реальных и потенциальных клиентах (их потребности, желания, предпочтения, увлечения, финансовые возможности, карьерные перспективы, изменения в семейном статусе и т.д.).

Цели и задачи предиктивной аналитики в определяющей мере фокусируются на том, чтобы предсказать, какой продукт, товар и услуга в какое время будут востребованы клиентами и за какую цену они могут быть приобретены. Для этого все шире используются системы ИИ, которые не только дают предсказания на основе обработки накопленных и непрерывно поступающих данных, но и в автоматическом режиме принимают решения по организации и реализации гибкой, подстраивающейся под клиента, маркетинговой политики, например, осуществляя адресную рассылку рекламы с предложениями льготных кредитов и привлекательных акций.

Используя технологический потенциал предиктивной аналитики в правоохранительной деятельности для профилактики преступлений, необходимо сформировать критерии выявления «клиентов», от которых можно ожидать те или иные преступления. Речь идет о лицах, совершающих правонарушения, замеченных в аморальных поступках, пьянстве, хулиганских выходках, употреблении наркотиков, бытовых скандалах, насилии, ранее судимых, рецидивистах, связанных с преступными сообществами, формирующих и поддерживающих криминальную субкультуру в сетевом эфире, подозреваемых в сопричастности к расследуемым преступлениям.

В таком клиентско-криминально ориентированном плане предиктивная оперативно-розыскная аналитика опирается непосредственно на модели и алгоритмы предиктивной криминологии, которые позволяют предсказывать преступления на основе накопления криминальных потенциалов личности, выявления индивидуальных криминальных кодов, и по существу, на основе анализа совокупности накапливаемых данных, позволяющих предсказывать действия и поступки человека.

Уже в ближайшей перспективе применение систем ИИ в предиктивной оперативно-розыскной аналитике должно быть направлено на автоматизацию выработки решений по организации и осуществлению профилактических мероприятий по предупреждению, предотвращению или пресечению возможных преступлений на разных стадиях формирования криминальных угроз.

10. Перспективы профилактики преступлений на базе открытых цифровых платформ

Борьба с преступностью в условиях цифровизации всех сторон жизни требует эффективного использования современных и перспективных средств информационно-психологических воздействий. Так, в цифровой трансформации правоохранительных структур выкристаллизовывается принципиально новая задача, а именно — подойти к созданию не только специализированных закрытых платформ, скажем, оперативно-розыскного назначения, а рассмотреть возможность формирования цифровых платформ открытой конфигурации, позволяющих по принципу социальных сетей привлекать определенную аудиторию граждан к сотрудничеству в профилактике и раскрытии преступлений, борьбе с криминальной идеологией, противодействию распространению криминальной субкультуры и, в целом, к обеспечению антикриминальной безопасности уже в «новом», цифровом мире.

Создание открытых цифровых платформ потребует не только технологических решений, организационного и правового обеспечения. Здесь на первый план выходят проблемы ментального содержания проектов, скажем, смыслового наполнения алгоритмов общения.

Необходимо представлять, что при всем многообразии задач, решаемых цифровой трансформацией (коммерция, услуги, производство, образование, медицина, логистика, управление, безопасность, борьба с преступностью), сверхзадача такой трансформации — это организация и управление социально-политическими

процессами, а в прикладном, правоохранительном плане — это декриминализация общественных отношений.

В «старом», доцифровом мире эта сверхзадача решалась силовыми средствами, экономическими мерами, психологическими воздействиями, применялись репрессии, принуждение, манипулирование. Цифровая трансформация очередной раз открывает возможность перехода на более высокие приоритеты управления: идеологический, исторический, мировоззренческий[1].

Для реализации такой возможности требуется фундаментальное исследование того, что будет основным инструментом управления в цифровом мире. Это сама информация. Но не та информация, которая обозначена как «данные и сведения независимо от формы их представления», и не то, что нам сообщают, не то, что мы слышим и видим. Речь идет об информации, которая рождается в сознании человека, возникает как функция целевой интерпретации получаемых сообщений, является необходимым компонентом реакций на воздействия и побуждения. Это реактивная информация, которая обеспечивает и жизненные процессы, и социальные отношения на всех уровнях — от передачи сигналов по нервным клеткам и встречи антител с вирусами до обмена комплиментами между супругами и дипломатическими нотами между государствами[2].

Именно реактивная информация накапливает потенциалы социальной энергии, т.е. энергии действий и поступков. Это могут быть потенциалы позитивной, созидательной энергии, а могут быть и потенциалы негативной, разрушительной энергии. Разрядка этой энергии приводит в движение массы людей и побуждает их к действиям и поступкам: от подвигов до преступлений[3].

Для управления социальными процессами необходимо создавать цифровые функциональные платформы, накапливающие необходимые энергоинформационные потенциалы, и цифровые инструментальные платформы, направляющие потоки социально-психологической энергии в нужное русло (рис. 8). И здесь на первый план выходит ментальное значение информационно-коммуникационных технологий и смысловое наполнение цифровых платформ

---

1 *Овчинский А.С., Борзунов К.К., Чеботарева С.О.* Информационные координаты. Управление. Противоборство. Безопасность. М.: Горячая линия — Телеком, 2018.

2 *Овчинский А.С.* Информационные воздействия и организованная преступность: курс лекций. М.: ИНФРА-М, 2007.

3 Там же.

безопасности, будь то информационная или антикриминальная безопасность[1].

Рис. 8. Функциональные и инструментальные цифровые платформы в управлении энергоинформационными трансформациями

С идеей создания открытых платформ вырисовываются контуры цифровой профилактики преступлений. Наряду с технологиями выявления лиц, представляющих угрозы общественной безопасности, необходима система целенаправленных воздействий на сознание тех людей, которые выходят на грань совершения преступления. Сегодня это актуально в первую очередь в профилактике высокотехнологичных преступлений, в обеспечении кибербезопасности, в противодействии экстремизму.

Особого внимания требует та криминальная среда, из которой выходят преступники, обладающие техническими средствами и, главное, навыками их применения в достижении своих криминальных амбиций.

И здесь профилактика преступлений вслед за высокотехнологичной преступностью и оперативно-розыскной деятельностью

[1] *Овчинский А.С., Борзунов К.К.* Энергоинформационные основы и приоритетные направления в борьбе с социальной деструкцией // Вестник Москов. ун-та МВД России. 2020. № 1. С. 138–144.

должна погружаться в виртуальные сферы, в которых «заваривается» и «кипит» «криминальное творчество».

Однако какими бы технологическими и криминальными навыками ни обладал потенциальный или уже состоявшийся преступник, он остается человеком. Хотя технологии искусственного интеллекта уже все чаще используются для совершения преступлений, роботы еще не открыли свой самостоятельный криминальный промысел. И пока преступник остается человеком, его сознание подвержено информационным воздействиям. Необходимость таких целенаправленных информационно-психологических воздействий, которые остановят потенциального преступника, разрушат криминальный замысел, а может быть, и вообще не дадут сформироваться и накопиться личностным криминальным потенциалам, требует создания открытых цифровых платформ, позволяющих не только осуществлять выявление объекта воздействия, но и активно управлять им.

А.В. Парфёнов

О перспективах развития розыскной и идентификационной деятельности в условиях цифровизации общества

В настоящее время подавляющее большинство экономически развитых стран и значительная часть развивающихся государств переходят в цифровой мир[1]. Стремительное развитие информационных технологий во всем мире, активное внедрение информационных разработок в повседневную жизнь человека заставляют правоохранительные органы работать над новыми, более совершенными методиками использования и применения передовых цифровых технологий для решения задач правоохранительных органов, в том числе и розыскной и идентификационной деятельности[2], в условиях формирования ИИ как способа развития умных технологий, роботов, «Интернета вещей»[3].

Необходимо обратить внимание на то, что опыт, полученный правоохранительной системой России и зарубежных государств в организации деятельности по решению задач по борьбе с преступностью в период пандемии 2020 г., позволяет сделать соответствующие выводы в выработке новых, совершенных подходов. В условиях пандемии заметно растет уровень киберпреступности[4].

Международные компьютерные сети (прежде всего информационно-телекоммуникационная сеть Интернет) призваны охватить практически все страны мира, благодаря чему открываются новые возможности в мировой экономике, политике, бизнесе, в сфере межличностных коммуникаций: появляются все новые способы об-

---

1 *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века. Международный опыт / под ред. С.В. Кузнецова. М.: Международные отношения, 2020. С. 16.

2 *Парфёнов А.В.* О сущности термина «розыскная и идентификационная деятельность» органов внутренних дел // Оперативник (сыщик). 2018. № 1 (54). С. 37–40.

3 *Пороховский А.А.* Цифровизация и искусственный интеллект: перспективы и вызовы // Экономика. Налоги. Право. 2020. № 13 (2). С. 84–91 [DOI: 10.26794/1999-849X-2020-13-2-84-91].

4 *Жданов Ю.Н., Кузнецов С.К., Овчинский В.С.* COVID-19: преступность, кибербезопасность, общество, полиция / вступ. ст. А.Л. Кудрина. М.: Международные отношения, 2020. С. 7–8.

щения как граждан между собой, так и с органами государственной власти. При этом развитие новых информационных технологий, формирование единой многоуровневой базы персональных данных, воплощение в жизнь идеи строительства электронного государства подчеркивают необходимость создания действенного механизма, обеспечивающего неприкосновенность сферы частной жизни человека, гарантирующего в том числе сохранность его персональных данных.

В настоящее время возрастает объем участия людей в обмене информацией, в том числе в электронном виде, при котором используются их персональные данные в рамках получения той или иной государственной, коммерческой либо другой услуги, что также становится фактором обеспечения социальной деятельности и эффективного общения. Причем большинство людей не имеют исчерпывающей информации о том, какие персональные данные, с какой целью, кому и в каком объеме передаются. Современный уровень развития и проникновения информационных технологий таков, что человек ежеминутно предоставляет огромное количество информации о себе самым различным компаниям. При этом мельчайшие частицы такой информации, включая кажущиеся совсем незначительными, могут комбинироваться друг с другом с помощью применения цифровых технологий, воссоздавая полный образ человека.

Цифровое присутствие неизбежно сосуществует с такими явлениями, как «цифровой след» и «цифровая тень».

Цифровая тень — это информация, создаваемая о людях автоматически посредством деятельности и устройств третьих лиц, а *цифровой след* — данные, самостоятельно передаваемые субъектом в цифровую среду, такие как электронные письма, регистрационные данные на сайтах социальных сетей, фотографии, геопозиции и т.п.

Интернет заполнен множеством цифровых следов и теней, которые могут использоваться для анализа поведения пользователя.

Вопросы обеспечения защиты от утечки информации и обеспечения безопасности информационной системы сводятся в том числе и к обеспечению информационной безопасности на социально-бытовом и личностном уровне. Методы и средства несанкционированного доступа к информационным ресурсам, основанные на особенностях психологии человека, использовании слабостей человеческого фактора, называют «социальной инженерией». Основной целью социальных инженеров является получение доступа к защищенным системам с целью кражи информации, паролей пользователей, данных о кредитных картах и т.д.

Желание поделиться своей радостью (знаменательные даты, события), успехами, а зачастую и обычное хвастовство заставляет человека отключить разумную часть своего сознания и не контролировать содержание выдаваемой им собственноручно информации при общении в социальных сетях.

Анализ информации, представленной человеком в социальных сетях, позволяет составить его морально-психологический портрет, узнать об увлечениях, семейном положении, обычаях, запланированных мероприятиях. Информация из социальных сетей, полученная в результате сбора и обработки, является исходной. В данном контексте предполагается трактовать понятие персональных данных максимально широко и причислять к ним любую информацию, относящуюся к определенному или определяемому лицу, — от транзакционных данных до перечня блюд в формуляре заказа завтрака в гостинице.

Важно отметить, что в случае с абсолютным большинством видов оборудования и программных продуктов речь идет о производстве неконтролируемого физическим лицом и недекларированного объема персональных данных. На следующем этапе необходимо осуществление планомерной деятельности по распространению персональных данных в интересах достижения конкретных целей лица, что может быть как самостоятельным процессом (например, размещение фотографий в социальных сетях), так и вспомогательным по отношению к главному (предоставление персональных данных для приобретения билетов, регистрации для получения доступа к публичной Wi-Fi сети и пр.).

При этом следует иметь в виду, что произведенные персональные данные в подавляющем большинстве случаев могут распространяться и вне зависимости от желания физического лица, например перепостом в социальных сетях или веб-сервисом по собственному решению. Отдельное внимание необходимо уделить производству персональных данных третьими лицами — смартфонами друзей, камерами городского видеонаблюдения, операторами баз данных и пр.

Общим правилом может служить допущение, что в непрерывном режиме ведется сбор данных физического лица, во многих случаях данный процесс является случайным, неосмысленным и неконтролируемым. Полученные персональные данные широко вводятся в оборот, и контроль их распространения физическим лицом практически невозможен. В связи с этим особое внимание целесообразно уделить именно процессу их производства и оказать на него максимально возможное влияние.

Цифровое присутствие на настоящем этапе развития цифровых технологий неоспоримо важно для эффективной деятельности человека, а также общения с другими людьми вне зависимости от их местонахождения. Благодаря цифровому присутствию человек сегодня выстраивает свои социальные связи и повышает комфорт условий жизнедеятельности вслед за развитием прогресса. Для формирования полноценного цифрового присутствия необходимо предоставление человеком своих персональных данных. При этом следует учитывать, что данная процедура может быть как контролируемой со стороны субъекта персональных данных, так и вынужденной, осуществляющейся без участия самого субъекта посредством деятельности и устройств третьих лиц.

В результате в этих двух случаях в цифровой среде возникает цифровой след (контролируемый) и цифровая тень (вынужденная), которые вместе формируют цифровой штамп человека и определяют его цифровое присутствие.

Информация, которую субъект персональных данных передает в цифровую среду, остается привязанной к источнику и идентифицирует его. Каждый «шаг» цифрового присутствия фиксируется, анализируется и позволяет определить субъекта, узнать новые сведения.

С каждым годом появляются все новые накопители и источники данных: датчики и носимые устройства, «умная» бытовая техника и др. Появляются новые сервисы и приложения, запрашивающие и собирающие данные о пользователях. Например, публичное размещение геолокации в сообщении позволяет обеспечить быстрое и удобное оформление заказа на сайте доставки товара и одновременно проинформировать о местонахождении субъекта.

Публичный профиль, в отличие от личного, может подразумевать использование некоего обнародованного псевдонима, общедоступного аккаунта в социальной сети и номера телефона, по которому может дозвониться любой желающий.

Разработка и применение современных методик распознания лиц, разыскиваемых правоохранительными органами, имеет на сегодняшний день важное значение в организации розыскной и идентификационной деятельности. Результаты исследования данной проблемы показывают, что правоохранительные органы технически развитых государств считают технологии распознания и нахождения людей фундаментальными.

Одна из таких методик — *автоматическое распознавание лиц* (*АРЛ*). Данная методика позволяет провести анализ особенностей лица, создать его математическую репрезентацию, сравнить ее

с базой данных имеющихся на соответствующих учетах лиц для определения возможных совпадений. Несмотря на результативность использования АРЛ, необходимо учитывать и некоторые реалии. Например, при использовании АРЛ на улицах городов в процессе осуществления розыскной и идентификационной деятельности необходимо учитывать постоянный людской поток, движение людей, которые не смотрят на установленные в общественных местах камеры, фокусирование которых может быть ослаблено в результате действия погодных условий (дождь, снег, туман и т.д.), загрязнения пылью и т.п.

Обращаясь к опыту зарубежных правоохранителей в использовании искусственного интеллекта, необходимо указать на перспективность данного направления. Так, в ходе эксперимента, проводимого в 2017 г., правоохранители Южного Уэльса (Великобритания) применяли АРЛ в двух режимах. Режим «Locate» применялся с использованием в реальном времени видеокамер, которые были размещены на полицейских специальных автомашинах и позволяли распознавать лиц по базам данных разыскиваемых и устанавливаемых подозреваемых[1]. Другой режим — «Identify» имел несколько иной принцип работы. Фотоизображения неустановленных преступников, изъятых с видеофиксаторов на местах совершенных преступлений, отождествлялись с имеющимися в базах данных фотоизображениями ранее привлекавшихся к уголовной ответственности лиц[2].

Результаты экспериментов показали, что за 12 месяцев исследований было задержано и арестовано более сотни лиц, подозреваемых в совершении тяжких и особо тяжких преступных деяний[3].

В ходе экспериментов были выявлены и недостатки, такие как невозможность работы систем в автоматическом режиме, в связи с чем сотрудникам полиции потребовалось адаптировать большинство стандартных процедур с целью достижения эффективности. Например, при выявлении влияния качества изображений на эффективность идентификационной работы системы для сотрудников, специализирующихся на работе с системами, возникла потребность в обучении использованию фото- и видеоизображений, пригодных для работы указанных систем.

---

1 На момент эксперимента в базе данных содержалось 600–800 фотоизображений разыскиваемых и идентифицируемых лиц.

2 База данных содержала около 450 000 изображений.

3 Как технология распознавания лиц помогает полиции // Хабр. URL: https://habr.com/ru/post/434280/ (дата обращения: 03.04.2021).

Проведенный анализ применения и использования систем распознания в городе Москве показал, что с 2017 г. на платформе городской инфраструктуры и с 2018 г. в метрополитене стартовала система распознания, по итогам внедрения которой ежемесячно задерживается от пяти до десяти разыскиваемых среди пассажиропотока в условиях Московского метрополитена, а с помощью использования полученной информации с видеокамер наружного наблюдения, установленных на жилых домах, за совершенные ими преступления было задержано более 90 лиц.

По данным департамента информационных технологий, представленным в правоохранительные органы данным аналитической работы с видеоматериалами столичного видеонаблюдения при проведении массовых мероприятий в 2018–2019 гг. органами внутренних дел было задержано 152 подозреваемых и обвиняемых[1].

В тестированиях и внедрении систем распознания на улицах и в метрополитене Москвы принимает участие «Центр речевых технологий», специализирующийся на биометрии. Кроме того, в данном проекте принимают участие компании «NtechLab» и «VisionLabs», которые предоставляют свои технологии.

Прежде чем рассматривать методики использования искусственного интеллекта в розыскной и идентификационной деятельности, необходимо раскрыть сущность одной из частей искусственного интеллекта — распознания изображений. Распознание и обработка изображений не тождественны. Обработка изображения означает преобразование самого изображения в форму цифр и математических операций с ними, в результате чего становится возможным получение дополнительной информации по изображению.

Обработка изображения состоит из следующих этапов: обработка цвета; оптимизация и улучшение качества изображения; получение внешне незаметных нюансов; реконструкция изображения; визуализация данных; захват, сохранение в цифровом виде и конвертация изображения; выявление специфики изображения[2].

Исходя из изложенного распознание изображений — это результат идентификации и отыскания объекта в цифровом изображении с использованием компьютерного зрения.

---

[1] МВД подвело итоги тестовой работы систем распознавания лиц в Москве // Ведомости. URL: https://www.vedomosti.ru/technology/articles/2019/06/26/805163-mvd-podvelo (дата обращения: 03.04.2021).

[2] *Исхаков М.* Что такое распознавание изображений и как ИИ помогает в их распознании? // Bezopasnik.info. URL: https://bezopasnik.info/что-такое-распознавание-изображений/ (дата обращения: 03.04.2021).

Процесс непосредственного распознавания изображений включает в себя:

— создание конструкций, иллюстрирующих объекты и особенности изображения, и их анализ, после чего данные ранжируются с извлечением нужной информации;

— создание прогнозирующей модели.

Искусственный интеллект открывает новые возможности распознавания образов. С помощью ИИ система распознавания лиц сравнивает особенности лица с изображениями и далее соотносит полученную информацию с массивом данных для получения возможных совпадений. Аутентификация лиц применяется производителями мобильных телефонов (например, как прием разблокировки смартфона), социальными сетями в интернет-пространстве (идентификация людей по изображению, при загрузке) и т.д. В настоящее время подобные системы вызывают вопросы, связанные с проблемой конфиденциальности, так как сбор данных возможен без согласия пользователей.

Одним из первых создателей систем распознания является доктор математики и физики Джозеф Атик, который в начале 90-х гг. прошлого столетия помог создать первые системы распознавания лиц. «Мы использовали статистический анализ, чтобы классифицировать черты лица как набор шаблонов, — рассказывает он. — Все сводилось к распознаванию образов. Во время сканирования лица обнаруживаются совпадения множества локальных особенностей — глаз, носа, уголков рта. Звучит как довольно примитивная технология, но на практике совокупность этих особенностей очень редко совпадает у двух людей»[1]. В последние 25–30 лет компьютерная техника получила возможность самостоятельно проводить данные операции при использовании постоянно совершенствующихся информационных систем глубокого обучения, базирующихся на «многослойном» программном обеспечении, построенном для распознания образов. Колоссальную базу данных для этого создают сами пользователи, которые размещают миллиарды фотографий в *Facebook*, *Google* и *Snapchat*.

Механизм работы рассматриваемых систем примерно следующий. После анализа видео или фото система преобразует данные в цифровой файл, который называют «отпечаток лица». В нем содержатся данные о характере черт лица и соотношениях

[1] Как устроен искусственный интеллект: распознавание лиц и бытовые мелочи // Популярная Механика. URL: https://www.popmech.ru/technologies/392532-kak-ustroen-iskusstvennyy-intellekt-raspoznavanie-lic-i-bytovye-melochi/ (дата обращения: 03.04.2021).

между ними. Программное обеспечение создает в общей сложности до 40 тыс. ключевых точек, но далеко не всегда существует необходимость все их использовать.

При этом в случае появления на лице бороды, смены прически система способна идентифицировать распознаваемое лицо. В нее заложены знания об изменчивости волосяного покрова, и он системой попросту исключается. Что действительно важно — так это треугольник лица: расстояние от виска до виска и от каждого виска до небольшого углубления под нижней губой[1].

Идентификация лиц нейронными сетями становится возможной, так как искусственные нейросети представляют собой математическую модель функционирования классических для живых организмов нейросетей — сетей нервных клеток. Как и в биологических системах, в искусственных нейросетях основным элементом выступают нейроны, объединенные между собой и составляющие слои, объем которых может быть разным в зависимости от сложности нейросети и ее назначения (стоящих перед ней задач).

Пожалуй, самая популярная задача нейросетей — распознавание визуальных образов. Сегодня создаются сети, в которых машины способны успешно распознавать символы на бумаге и банковских картах, подписи на официальных документах, детектировать объекты и т.д. Эти функции позволяют существенно облегчить труд человека, а также повысить надежность и точность различных рабочих процессов за счет исключения ошибки, возможной из-за человеческого фактора.

Нейросеть — это математическая модель в виде программного и аппаратного комплекса, строящаяся на принципах функционирования биологических нейросетей. Сегодня такие сети активно используют в практических целях из-за возможности не только разработки, но и обучения[2]. Их применяют для прогнозирования, распознавания образов, машинного перевода, распознавания аудио и т.д.

Обучение нейросетей осуществляется сегодня многими компаниями по всему миру. В России разработками в этой сфере заняты, к примеру, «Яндекс», а также производители «Сколково», МФТИ и ВШЭ.

---

[1] Как устроен искусственный интеллект: распознавание лиц и бытовые мелочи // Популярная Механика. URL: https://www.popmech.ru/technologies/392532-kak-ustroen-iskusstvennyy-intellekt-raspoznavanie-lic-i-bytovye-melochi/ (дата обращения: 03.04.2021).

[2] Что такое нейронная сеть: кратко // Центр 2М. URL: https://center2m.ru/ai-recognition (дата обращения: 03.04.2021).

Компания «Центр 2М» разработала и успешно внедряет систему промышленной видеоаналитики «CenterVision», которая использует нейросети для распознавания объектов на предприятиях с точностью до 98%.

В 2015 г. отечественная компания «Youth Laboratories» организовала первый в мире конкурс красоты, в котором красота участников оценивалась только нейросетями, учитывающими множество особенностей внешности.

Цена современных систем распознавания разнится, однако из-за высокой трудоемкости создания функциональных и эффективных нейронных сетей, а также их обучения, доступ к ним обычно требует немалых финансовых вложений. В большинстве случаев применение систем распознавания возможно по лицензии от производителя, цена которой (в зависимости от функционала) составляет от нескольких тысяч до десятков тысяч долларов.

Необходимо также обратить внимание на то, что автоматическая обработка персональных данных позволяет оценить определенные личные характеристики физического лица, в том числе для анализа или прогнозирования его характеристик, касающихся производительности труда, экономического положения, здоровья, личных предпочтений и интересов, добросовестности, поведения, местоположения и перемещений.

Практически все устройства находятся под управлением нескольких наиболее распространенных операционных систем. Среди этих устройств — смартфоны, телевизоры, настольные компьютеры и ноутбуки, планшетные компьютеры, автомобили и др.

Нейронные сети находят самое разное применение, причем не только при распознавании изображений и текстов, но и во многих других сферах. Они способны к обучению, благодаря чему нейронные сети можно оптимизировать и максимально увеличивать их функциональность.

Исследование нейронных сетей в настоящее время является одной из самых перспективных областей, поскольку в будущем они будут применяться практически повсеместно, в разных областях науки и техники. Это связано с тем, что нейронные сети способны значительно облегчить труд, а иногда и обезопасить человека. Правоохранительные органы, имея на вооружении методики использования искусственного интеллекта, смогут реализовать эффективный подход к организации розыскной и идентификационной деятельности в Российской Федерации.

Ю.А. Лапунова, А.Ю. Бегунов

Полемика о концептуальных основах цифровой оперативно-розыскной деятельности

Информационное общество[1], цифровая экономика[2], цифровое государственное управление[3], цифровые технологии[4], цифровые права[5], цифровая безопасность[6], цифровая преступность[7], циф-

[1] Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы» (действующая редакция) (СПС «КонсультантПлюс»).

[2] Паспорт национального проекта «Национальная программа “Цифровая экономика Российской Федерации”», утв. президиумом Совета при Президенте РФ по стратегическому развитию и национальным проектам, протокол от 4 июня 2019 г. № 7 (действующая редакция) (СПС «КонсультантПлюс»).

[3] Паспорт Федерального проекта «Цифровое государственное управление», утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28 мая 2019 г. № 9 (действующая редакция) (СПС «КонсультантПлюс»).

[4] Паспорт Федерального проекта «Цифровые технологии», утв. президиумом Правительственной комиссии по цифровому развитию, использованию информационных технологий для улучшения качества жизни и условий ведения предпринимательской деятельности, протокол от 28 мая 2019 г. № 9 (действующая редакция) (СПС «КонсультантПлюс»).

[5] Статья 141.1. Цифровые права // Гражданский кодекс Российской Федерации (часть первая) от 30 ноября 1994 г. № 51-ФЗ (действующая редакция) (СПС «КонсультантПлюс»).

[6] Например, см.: Цифровая безопасность личности, общества и государства в условиях глобализации: юридические механизмы обеспечения. Обзор сессии в рамках ПМЮФ 2019 г. / А.И. Овчинников, О.В. Ахрамеева, С.А. Воронцов и др. // Вестник юридического факультета ЮФУ. 2019. Т. 6. № 2. С. 111–122; *Тарасенкова А.Н.* Информационное право: возрастная маркировка, цифровая безопасность и другие вопросы. М., 2019; *Ахрамеева О.В.* Нотариальный механизм обеспечения цифровой безопасности прав граждан и юридических лиц в условиях цифровизации // Нотариус. 2020. № 1; *Лебедев С.Я.* Цифровая безопасность — цифровой уголовно-правовой ресурс // Криминология: вчера, сегодня, завтра. 2019. № 4 (55). С. 17–25.

[7] *Ищук Я.Г.*, *Пинкевич Т.В.*, *Смольянинов Е.С.* Цифровая криминология: учеб. пособие. М.: Академия управления МВД России, 2021. С. 129–147; *Поляков И.В.* Цифровая преступность: проблемы понятийного аппарата, систематизации и правоприменительной практики // Проблемы правоохранительной деятельности. 2020. № 2. С. 21–25.

ровая информация[1] и т.п. Кардинально меняющаяся картина мира, или, иными словами, складывающаяся оперативная обстановка в условиях цифровизации, новых вызовов и угроз, ставит перед авторами ряд проблемных вопросов, поиск научно обоснованных и практикоориентированных ответов на которые они предпримут попытку осуществить в настоящей статье.

Своевременно ли говорить о начале реализации концепции цифровой полиции[2]? Кто он, «цифровой оперуполномоченный», в контексте цифровой полиции?

Имеем ли мы уже сейчас достаточные научно-практические предпосылки для формирования теории цифровой ОРД как ключевого инструмента в противодействии преступности в целом?

Авторы предпримут попытку аргументированно и последовательно представить позицию по обозначенным вопросам.

1. Сегодня можно с полной уверенностью сказать, что для решения стоящих перед ОВД, да и в целом перед правоохранительными органами, задач по борьбе с преступностью требуются высокотехнологичные решения. Ключевой перелом, заключающийся в первую очередь в осознании необходимости цифровой оптимизации обеспечения деятельности ОВД Российской Федерации, наступил в 2019 г., когда были определены концептуальные основы цифровой полиции[3], единого цифрового информационного пространства, оснащения полицейских перспективными электронными средствами, разработки робота-полицейского. Вместе с тем следует констатировать, что цифровая полиция подразумевает в настоящее время разработку и внедрение высокотехнологичных решений и не охватывает пласт человеческой эволюции, цифрового полицейского — человека. Однако, изучая зарубежный опыт в рассматриваемой сфере, опыт крупных коммерческих структур по выявлению и нейтрализации цифровых инцидентов[4], авторы пришли

---

1 Например, *Бегишев И.Р.* Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук. Казань, 2017; *Иванов Н.А.* Криминалистические классификации цифровой информации // Вестник Омской юридической академии. 2013. № 1 (20). С. 81–84.

2 *Конуров А., Конюшев В., Абрамов М.* Создание и развитие концептуального облика цифровой полиции // Профессионал. 2019. № 5. С. 2–5.

3 Там же.

4 *Овчинский В.С.* Технологии будущего против криминала («Коллекция Изборского клуба»). М.: Книжный мир, 2017; *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. М.: Международные отношения, 2020.

к выводу, что в корне должен меняться подход к подбору, воспитанию и обучению цифрового полицейского — человека, стоящего на страже борьбы с преступностью.

Общеизвестен факт, что на передней линии борьбы с преступностью, в том числе цифровой, стоит оперативный сотрудник любого оперативного подразделения органа, осуществляющего ОРД. Анализ решения Коллегии МВД России от 1 ноября 2019 г. № 3км, объявленного приказом МВД России от 25 ноября 2019 г. № 878, подтверждает данный тезис.

Итак, кто он — *цифровой оперативный сотрудник*? Набором каких компетенций он должен обладать уже сегодня?

Проведенные авторами исследования показали, что данные сотрудники отличаются (должны отличаться) разносторонним развитием, высоким уровнем образованности и обладают набором:

- знаний в сфере юриспруденции (при этом особого внимания заслуживают знания уголовно-правового, криминологического характера, нормативно-правового регулирования вопросов цифровизации и, несомненно, методик выявления, предупреждения и раскрытия преступлений, совершаемых как с использованием ИТК, так и непосредственно в информационно-телекоммуникационной среде, соблюдения принципа конспирации при решении задач ОРД в цифровом пространстве), в высокотехнологичной сфере (цифровых инструментов, услуг), в области психологии (особенно при работе в закрытых группах (сообществах) с использованием ИТК);
- умений работать с большими данными, цифровой информацией;
- навыков алгоритмизации действий по выявлению, своевременному недопущению либо раскрытию преступлений и иных правонарушений, а также осуществления ОРД в цифровом пространстве.

При этом немаловажными составляющими характеристики оперативного сотрудника нового формата являются его ориентированность на саморазвитие, постоянный поиск и изучение новых трендов цифрового мира, позволяющих работать на опережение преступного элемента. Кроме того, необходимо выявлять и поддерживать у сотрудника соответствующую мотивацию на достижение результата — эффективного и положительного воздействия на «чистоту» цифрового пространства.

И вместе с тем оперативник настоящего и тем более будущего должен осознавать всю ответственность того, что именно он выступает от лица государства гарантом защиты личности, общества и государства от преступных проявлений в цифровой среде.

Не вызывает сомнений, что это лишь минимум компетенций, которыми должен обладать цифровой оперативный сотрудник.

Безусловно, при таком наборе компетенций немаловажную роль играют общие и специфические личные характеристики данного сотрудника[1] и, в частности, мотивация поступления на службу. Поскольку каждый подобный высококлассный специалист в случае смещения ориентиров может нанести очень серьезный ущерб личности, обществу и государству.

2. В настоящее время наблюдается глубокий разрыв между скоростью развития цифровых технологий и нормативно-правового регулирования вопросов цифрового пространства, научно-практических обоснований технологических прорывов и морально-этических норм.

Несомненно, данные противоречия характерны также для осуществления защиты личности, общества и государства в цифровом пространстве посредством применения такого инструмента уголовно-правового характера, как ОРД.

Не вдаваясь в частные теории ОРД в цифровом пространстве, авторы пришли к заключению, что ключевой массив научных работ, внесших и вносящих глубокий вклад в развитие теории ОРД в целом, а также создающих предпосылки к формированию теории цифровой ОРД как особого (специального) научного направления теории ОРД, можно условно разделить на следующие группы:

— научные работы, в том числе диссертационные исследования, посвященные проблематике ОРД по противодействию преступлениям, совершаемым с использованием ИТК, а также в сфере ИТК (в том числе по отдельным видам преступлений)[2];

— научные работы, предметом изучения которых является в целом киберпространство (цифровое пространство) как особая среда осуществления ОРД[3];

— научные работы, в том числе диссертационные исследования[4] в области уголовного права;

---

[1] Более подробно это будет рассмотрено в последующих научных работах.

[2] К работам, отражающим сущностные особенности противодействия преступлениям, совершаемым с использованием информационно-телекоммуникационных технологий, однозначно следует отнести научные изыскания А.Л. Осипенко.

[3] К примеру, см.: Теория оперативно-розыскной деятельности: учебник / под ред. К.К. Горяинова, В.С. Овчинского. 5-е изд., испр. и доп. М.: ИНФРА-М, 2021. С. 368–389.

[4] Ярким примером, отражающим рассматриваемую специфику, являются научные взгляды Е.А. Русскевича.

— научные работы в области криминологии, в рамках которой в настоящее время глубоко изучаются цифровая безопасность[1], цифровая преступность[2] и цифровая криминология[3];

— научные работы, предметом изучения которых являются различные цифровые решения[4];

— иные научные работы, опосредованно оказывающие влияние на возможное развитие теории цифровой ОРД[5].

Анализ значимого количества научных работ из каждой выделенной авторами группы позволил прийти к ряду умозаключений.

1. Учеными обоснованы предложения по специфике организации, тактики и методики осуществления ОРД в целях противодействия IT-преступности.

2. Требуется качественно иное ресурсное обеспечение оперативно-розыскной деятельности, осуществляемой в цифровом пространстве.

3. Необходимо сформировать принципиально новую систему подготовки кадров по данному направлению (от специализированных классов уже в школах до трудоустройства и регулярных повышения квалификации и переподготовки).

4. Цифровое пространство является специфической средой осуществления ОРД, и ее ключевые элементы принципиально отличаются от осуществления ОРД в физической среде.

5. Поскольку криминологическая характеристика является одним из ключевых элементов оперативно-розыскной характеристики преступления, мы можем с уверенностью говорить о том, что основные положения научного знания цифровой криминологии могут быть положены в основу научного знания о цифровой ОРД.

6. Цифровая ОРД — важнейший инструмент уголовно-правового характера по обеспечению цифровой безопасности.

---

[1] Например, см.: Цифровая безопасность личности, общества и государства в условиях глобализации: юридические механизмы обеспечения. Обзор сессии в рамках ПМЮФ 2019 г. / А.И. Овчинников, О.В. Ахрамеева, С.А. Воронцов и др. // Вестник юридического факультета ЮФУ. 2019. Т. 6. № 2. С. 111–122.

[2] *Ищук Я.Г.*, *Пинкевич Т.В.*, *Смольянинов Е.С.* Цифровая криминология: учеб. пособие. М.: Академия управления МВД России, 2021.

[3] Там же.

[4] Примером могут служить научные работы А.И. Филиповой в сфере правового регулирования искусственного интеллекта.

[5] Безусловно, к таким научным работам в первую очередь мы относим научные исследования в области оперативно-розыскной деятельности, криминологии, уголовного права, уголовного процесса.

7. Непременно должна быть разработана и научно обоснована принципиально иная система оценки деятельности оперативных подразделений правоохранительных органов, базирующаяся на создании системы обеспечения недопущения совершения противоправных деликтов посредством своевременного устранения обстоятельств, способствующих совершению преступлений, а также преступных действий конкретного лица в цифровом пространстве на основе глубокого анализа больших данных и последующих результатов прогнозирования, пресечения преступлений, предупреждения нанесения материального ущерба личности и государству на основе прогнозирования и выработки маркеров (алгоритмов), свидетельствующих о возможных угрозах и рисках.

Несомненно, решение этих задач позволят обеспечить технологии ИИ, развитию которых в системе МВД России в настоящее время уделяется очень серьезное внимание со стороны непосредственно руководства МВД России. Свидетельствами, подтверждающими данный тезис, служат поручения о разработке Концепции научно-технической политики МВД России, *Концепции использования искусственного интеллекта в деятельности органов внутренних дел*, а также проведение ГИАЦ МВД России совместно с Академией управления МВД России уже ставшей традиционной ежегодной Международной научно-практической конференции «Искусственный интеллект на службе полиции».

Несмотря на то, что были рассмотрены только отдельные ключевые позиции, свидетельствующие о трансформации (эволюции) ОРД, осуществляемой в цифровом пространстве, позволим себе сделать смелый вывод о том, что уже созданы научно-практические предпосылки формирования теории цифровой ОРД как специфической и относительно самостоятельной отрасли научного знания, требующей дальнейшего развития и обоснования.

Г.Г. Саркисян

Особенности подготовки аналитиков для подразделений, осуществляющих информационно-аналитическое обеспечение оперативно-розыскной деятельности органов внутренних дел Российской Федерации

Повышение эффективности информационного и аналитического обеспечения деятельности органов государственной власти является одной из приоритетных задач, стоящих перед ними. Соответственно, качественные показатели ее выполнения напрямую отражаются на военной, политической, экономической и социальной стабильности в обществе. В интересах выполнения своей миссии информационно-аналитическими подразделениями различных государственных органов, учреждений и ведомств осуществляются сбор, обработка и анализ больших массивов данных. В качестве источников при этом выступают национальные, зарубежные и международные информационные ресурсы, органы государственного и муниципального управления, а также другие субъекты и подразделения, непосредственно осуществляющие сбор, обработку и анализ представляющей интерес информации.

С учетом современных тенденций в условиях перехода к цифровой экономике и всеобщей информатизации общества анализ больших массивов данных является неотъемлемой частью деятельности ОВД и требует перераспределения кадровых, финансовых и технологических ресурсов. В свою очередь, для обеспечения эффективной деятельности информационно-аналитических подразделений, как, впрочем, и множества других, прежде всего необходимо укомплектование их профессиональными кадрами, поскольку развитие и широкое использование информационных технологий требует привлечения новой категории сотрудников — аналитиков.

В российских образовательных организациях высшего образования еще не выстроена эффективная система подготовки такого класса специалистов, а большинство имеющихся сотрудников являются в данном деле самоучками, которые приобрели профессиональные качества в силу своих специфических особенностей

личности и склада ума, а также склонности к аналитической работе[1].

Вновь появившаяся профессия уже стала наиболее важной и востребованной на рынке труда среди специальностей, обеспечивающих перспективу и условия для развития организации или государственного органа. Спрос на рынке труда уже обеспечил реализацию таких профессионалов, как системный аналитик, финансовый аналитик, кредитный аналитик, бизнес-аналитик, бюджетный аналитик, инвестиционный аналитик, аналитик-преподаватель и др. Вместе с тем появление новой профессии повлекло за собой новые вызовы и проблемы, связанные в первую очередь с подготовкой, переподготовкой и совершенствованием профессиональной деятельности аналитиков.

Образовательные организации высшего образования не занимаются подготовкой аналитиков в том числе потому, что в государственных образовательных стандартах направление «аналитик» не закреплено. Несмотря на это, подготовку, переподготовку и повышение квалификации сотрудников в сфере общих методов аналитической деятельности взяли на себя частные компании, предоставляющие услуги в области образования.

Аналитик — это специалист с логическим типом мышления, способный к анализу и синтезу информации, обладающий отличной памятью, умением обращать внимание на детали, способный отфильтровывать из огромного информационного потока нужную информацию, выделять из нее те сведения, которые могут послужить основанием для существенных выводов. Другими словами, преобладающими для такого специалиста являются аналитические способы деятельности[2].

Задачей аналитика является «возвышение» над проблемой, что необходимо для того, чтобы увидеть те ее особенности, которые скрыты при рассмотрении «неподготовленным» взглядом. Это всегда сложно из-за жесткого цейтнота, в котором протекает изучение объекта интереса.

Предполагается, что аналитик при осуществлении своей деятельности представляет все вариации и модификации «большой картинки», в том числе в случае, когда он не является экспертом

---

[1] См.: *Саркисян Г.Г.* Аналитическая работа оперативных подразделений органов внутренних дел // Сборник материалов Международного конкурса на лучшую научную публикацию молодых ученых. 2018. С. 148–151.

[2] См.: *Монахова Л.Ю., Монахова А.А.* Формирование специалиста-аналитика на основе информационно-тренинговых технологий // Человек и образование. 2008. № 2 (15). С. 50–53.

в этой области. Можно сказать, что основная цель данного вида деятельности — своего рода прогнозирование и предугадывание того, что в конечном итоге будет нужно и полезно «заказчику» информации.

В связи с изложенным справедливым является вопрос, какими профессиональными знаниями и навыками должен обладать аналитик и какие из них необходимы для организации и эффективного осуществления аналитической деятельности? Чтобы ответить на этот вопрос, необходимо обратиться к самой сути аналитической деятельности. Осуществляемый аналитиком процесс анализа включает в себя последовательное выявление заложенных ранее опытным путем и при получении новой информации ассоциативных рядов и взаимосвязей. Поэтому именно те свойства, которые помогают качественному осуществлению данного процесса, и являются ключевыми для аналитика.

С учетом сказанного, а также на основе проведенного анализа установлено, что такими качествами выступают память, внимание, скрупулезность, скептицизм и критическое мышление.

- *Память* — способность сохранять и при необходимости воспроизводить полученную информацию. Память — одно из важнейших свойств аналитика. Именно благодаря памяти человек может накапливать знания (в том числе опыт) и использовать их для изучения новой информации.
- *Внимание* — способность не пропустить ни одной детали и замечать, казалось бы, незначительные, не важные на первый взгляд элементы.
- *Скрупулезность* также имеет огромное значение, поскольку аналитику приходится работать с огромным количеством небольших и неприметных объектов (элементов информации).
- *Скептицизм*, базирующийся на сомнении и перепроверке, является основой. Но поскольку достоверность всей информации проверить невозможно, склонность к сомнению не должна переходить определенные границы.
- *Критическое мышление* — один из основных навыков современности, который позволяет анализировать информацию с последующей выработкой выводов и принимаемых на их основе решений, а также формировать собственное мнение и отстаивать свою позицию.

  Человек, обладающий критическим мышлением, способен:

  — понимать логические и причинно-следственные связи между разными идеями и понятиями;

— быстро анализировать суждения окружающих и оценивать их;

— грамотно конструировать собственные аргументы и доносить их до окружающих;

— замечать нестыковки, несоответствия и тривиальные ошибки в логике и аргументации;

— отмечать важность и релевантность идей общему контексту;

— рефлексивно оценивать собственные мнения и верования.

Исходя из изложенного, вариативным компонентом в модели подготовки специалиста-аналитика является наличие знаний в области конкретной профессиональной деятельности, которую он обеспечивает. Он должен свободно владеть и грамотно применять на практике технологии статистических и экономико-математических исследований, обладать навыками использования инструментов, позволяющих их реализовать при решении конкретной задачи с последующим прогнозированием с определенной степенью точности дальнейшего развития исследуемых процессов или явлений. Такими инструментами являются статистические методы, нашедшие свое отражение в информационно-праксиологических средах — пакетах прикладных программ. В связи с этим целью формирования умений в аналитической деятельности специалиста становятся обучение и обогащение его современным теоретико-прикладным инструментарием в области информационно-прогностических исследований[1].

Общеизвестно, что обучение — ключевой фактор прогресса для любой организации. Правоохранительные органы и входящие в них оперативные подразделения не являются исключением. Как известно, в МВД России внедрена платформа информационно-телекоммуникационной системы (ИСОД) ОВД, которая объединяет различные базы и информационные системы в некоторое единое пространство. Это позволяет сотрудникам правоохранительных органов использовать весь объем накопленных данных в своей повседневной деятельности, связанной в том числе с информационно-аналитическим обеспечением ОРД.

В настоящее время большинство подразделений ОВД располагают автоматизированными информационными системами, функционал которых позволяет осуществлять учет результатов оперативно-служебной деятельности, организовывать профессио-

[1] См.: *Монахова Л.Ю.* Информатизация математического образования в системе профессиональной подготовки военных специалистов: дис. ... д-ра пед. наук. Великий Новгород, 2005.

нальную деятельность и готовить управленческие решения. Такими возможностями в той или иной степени обладают органы полиции всех современных государств, а статистические данные и результаты их анализа ложатся в основу принятия управленческих решений и прогнозирования полицейской деятельности. И как следствие, основанные на аналитических инструментах прогнозы позволяют избрать эффективный курс противодействия преступной деятельности и рассчитать оптимальные комбинации применения сил и средств[1].

Что касается организации деятельности оперативных подразделений органов внутренних дел, то, помимо технических аспектов решения проблемы информатизации, назрела и проблема подготовки специалистов-аналитиков (оперативников-аналитиков). Причем немалую роль в этом вопросе играет все еще низкий уровень информационной культуры пользователей информационно-телекоммуникационных сетей и информационных систем[2].

Информационная культура является частью профессиональной культуры современности, причем не только для аналитиков, но и для многих других специальностей. Она представляет собой систему полученных знаний, умений, навыков и правил в области информационно-аналитической деятельности, которые позволяют ее пользователю свободно ориентироваться в информационном пространстве, осуществлять сбор, обработку информации, а также использовать независимо от местонахождения необходимые ему сведения, материалы и документы. Кроме того, она включает в себя и владение навыками в сфере применения методик и технологий работы с информацией, а также организации ее поиска, сбора, обработки, распределения и анализа, с последующим представлением результатов.

Составляющими информационной культуры являются следующие навыки:

— поиска и отбора новой информации;

— переработки и структурирования больших массивов информации;

---

[1] См.: *Степанян А.И.* Предиктивная аналитика в прогностической деятельности полиции современных государств // Вестник СПб. ун-та МВД России. 2019. № 4 (84). С. 43–50.

[2] См.: *Саркисян Г.Г.* Информационное обеспечение деятельности оперативных подразделений органов внутренних дел // Труды Академии управления МВД России. 2018. № 2 (46). С. 167–169.

— использования существующих и создания и ведения собственных баз данных для решения повседневных и оперативно-розыскных задач;

— использования телекоммуникационных каналов связи при решении служебных задач;

— четкого и понятного изложения результатов аналитической деятельности, в том числе посредством использования современных информационных технологий[1].

Следующим важным аспектом является сама информационно-аналитическая работа. В данном контексте анализ представляет собой последовательный процесс, предусматривающий поэтапное выполнение аналитиком действий для получения желаемого результата. Такими действиями выступают сбор и обработка данных, их оценка, распределение и систематизация, анализ и представление информации заказчику. Инструментарий, который при этом используется, должен соответствовать реализуемым аналитическим методикам. В свою очередь, тем более качественные аналитические результаты будут получены, чем более интегрированный инструментарий был при этом использован.

Аналитические технологии — это методики, которые на основе каких-либо моделей, алгоритмов, математических теорем позволяют по известным данным оценить значения неизвестных характеристик и параметров.

Как правило, в качестве инструментов аналитической деятельности выступают специальные персональные решения, которые имеют весьма ограниченный функционал по обеспечению безопасности или не имеют его вовсе. Вместе с тем организация доступа к имеющимся в распоряжении информационным источникам и ресурсам в сети должна в обязательном порядке включать в себя соответствующий уровень безопасности. Поэтому все используемые информационно-аналитические системы должны обладать возможностью использования технологии шифрования паролей для каждого из пользователей, а также возможностью контроля режимов и уровней доступа к ресурсам, копирования и передачи информации.

Такое построение работы особенно важно при организации и построении закрытых каналов передачи информации в территориально-распределенных системах оперативных подразделений,

[1] См.: *Хижняков Д.П.* Информационно-аналитические службы и их деятельность по обеспечению процесса принятия решений в региональных органах власти // Молодой ученый. 2010. Т. 1. № 1–2. С. 263–266.

которые предусматривают информационно-аналитическое взаимодействие, в том числе на межведомственном уровне[1].

Следует также согласиться с мнением профессоров Н.В. Павличенко и А.И. Тамбовцева о том, что под влиянием процессов, протекающих сегодня в обществе, профессия оперативного уполномоченного значительно трансформируется от традиционного оперативного уполномоченного — коммуникатора к оперативному уполномоченному — аналитику Big Data[2].

Кроме того, необходимо обратить внимание на негласный характер самой ОРД и, соответственно, ее аналитической составляющей. Так, учеными В.В. Загайновым и Ю.Н. Кононовым отмечается, что оперативно-аналитическая работа оперативных подразделений имеет характерные особенности, выделяющие ее на фоне других видов криминального и криминогенного анализов. К таковым относятся: специфические субъекты, особенности формирования информационной системы, цели, задачи, объекты и предмет исследования, преимущественно непроцессуальный характер, а также средства, формы, методы и способы осуществления данной деятельности[3].

Представляется, что будущие офицеры информационно-аналитических подразделений органов внутренних дел должны уметь:

— решать информационно-аналитические и статистические задачи с применением общего и специального программного обеспечения;

— осуществлять анализ и прогнозирование криминогенных явлений и процессов.

Для этого им необходимо знать:

- основные принципы и порядок сбора, обработки, структуризации, анализа и прогноза статистических и оперативных данных;
- сущность и методы построения основных статистических и информационно-аналитических моделей;

---

1 См.: *Иванов П.Ф.* Информационно-аналитическое обеспечение региональных органов власти и управления // Аналитический вестник Совета Федерации ФС РФ. 2002. № 2 (157). С. 23–43.

2 См.: *Павличенко Н.В., Тамбовцев А.И.* Будущее профессии оперуполномоченный — Big Data и аналитика // Труды Академии управления МВД России. 2020. № 2 (54). С. 62–68.

3 См.: *Загайнов В.В., Кононов Ю.Н.* Оперативно-аналитическая работа как основа оперативно-розыскной деятельности в современных условиях// Вестник Восточно-Сибирского института МВД России. 2017. № 1 (80). С. 37–45.

- технические комплексы и программное обеспечение, используемые для организации информационно-аналитической работы[1].

В заключение следует подчеркнуть, что в условиях всеобщей цифровизации подготовка аналитиков на государственном уровне, причем как в общих, так и в специализированных образовательных организациях высшего образования, готовящих сотрудников органов внутренних дел, становится первоочередной задачей. Такая подготовка должна включать в себя стратегическое и оперативное аналитическое обучение. Аналитикам предстоит пройти сложное обучение, чтобы понять роль и функции анализа преступной деятельности в правоохранительных органах, законодательную базу и современные нормативные правовые требования, предъявляемые к различным методикам и технологиям сбора, обработки и анализу информации, а также ее обмену и использованию. Подготовку аналитиков следует организовать в несколько этапов, а также с учетом уровня и функционала должностей. В этот процесс необходимо также включить получение знаний и навыков по сбору, обработке и структурированию полученной информации, с последующим проведением детального анализа, построению на его основе выводов и формулированию методических рекомендаций. Именно поэтому в процесс подготовки аналитиков входит получение следующих обязательных навыков: написание и подготовка отчетов; объединение в единый процесс оперативно-аналитической деятельности и ОРМ, а также анализ и последующее принятие на его основе решений. Кроме того, необходимы знание методов и технологий анализа, инструментов, технических средств и программных продуктов анализа данных, источников информации, соответствующих этим задачам нормативной правовой основы и правоохранительной этики, а также умение применять их.

---

[1] См.: *Корнеев В.В.* Организация информационного обеспечения органов исполнительной государственной власти // Северный регион. 2003. № 2 (8). С. 159–164.

Ю.Н. Жданов, В.С. Овчинский

Возможности видеонаблюдения для оперативно-розыскной деятельности

«Новая нормальность» эпохи пандемии, связанная с беспрецедентным расширением использования технологий видеонаблюдения, геолокации и Big Data, создает возможности их эффективного применения в оперативно-розыскной деятельности.

Опыт Москвы

Считается, что современная система видеонаблюдения в рамках программы ***«Безопасный город»*** в Москве появилась в 2011–2012 гг. До этого она была довольно архаичной, использовалась неэффективно, многие камеры просто не работали.

В качестве ориентира и ролевой модели для Москвы был выбран ***Сингапур*** — в этом городе-государстве строилась система «умного города», которая была запущена в 2014 г. Она, например, включала в себя разветвленную сеть камер видеонаблюдения и установленные во все машины датчики, позволяющие оперативно собирать данные о пробках.

Власти Сингапура продемонстрировали и другие чудеса новой системы. В 2013 г. они показательно оштрафовали на 14 тыс. долл. человека, который выбрасывал окурки из окна квартиры: его выявили вездесущие камеры наблюдения, писал *Wall Street Journal*.

С начала реализации проекта количество видеокамер увеличивалось примерно на 7–10 тыс. в год. В мае 2019 г. мэр Москвы Сергей Собянин сказал, что в Москве их 167 тыс. (к началу 2021 г. — уже около 200 тыс.). Мэр добавил, что ***видеозаписи оттуда используются при расследовании 70% всех совершенных преступлений***.

Большинство камер установлены у подъездов жилых домов и административных зданий, в школах, вузах, торговых центрах. Не менее 2,5 тыс. камер установлены в местах массового скопления людей.

Чаще всего записи с видеокамер используются для расследования вандализма или краж (в 52% случаев) и для разбора ДТП (в 40% случаев).

Для Москвы была выбрана российская технология от компании ***NTechLab***, которая в свое время разработала FindFace — не рабо-

тающий сейчас портал для поиска людей во «ВКонтакте» по изображению. Нейросеть NTechLab позволяет обнаружить четырех из пяти разыскиваемых, лица которых хоть раз были зафиксированы хотя бы одной камерой, а время поиска человека в базе из 1 млрд снимков занимает не более 10 секунд, следует из презентации компании.

В тестовом режиме система работала ***в 2017 и 2018 гг. во время Кубка конфедераций и Чемпионата мира по футболу в Москве***. По официальной версии — чтобы выявлять болельщиков из черного списка, которым запрещен проход на стадионы. Тестирование системы распознавания лиц началось в Москве в августе 2017 г. — сначала на 1500 камерах. Во время чемпионата мира по футболу в 2018 г. на входах на стадионы и фестиваль болельщиков работали уже более 450 специальных камер, которые автоматически сверяли лица всех заходящих с предварительно загруженной базой из 45 тыс. фотографий. За время чемпионата было задержано 19 человек, находившихся в федеральном розыске, и 49 человек, которых власти отнесли к опасным футбольным фанатам.

Гонка Москвы за покрытием видеокамерами всего пространства города не является уникальной. По данным организации *Caught on Camera* (она на протяжении 30 лет занимается разработкой систем видеонаблюдения по заказу государственных и коммерческих структур), в ***Лондоне*** и населенных пунктах вокруг него установлено 500 тыс. видеокамер, т.е. в два с половиной раза больше, чем планируется оборудовать в Москве.

Россия по числу установленных камер для видеонаблюдения заняла третье место в мире, уступив Китаю и США, говорится в исследовании информационного аналитического агентства *TelecomDaily*.

Сегодня в России насчитывается около 13,5 млн камер, в то время как в Китае их 200 млн, в США — 50 млн. По числу камер на 1 тыс. человек при этом лидирует США (152,8 камеры), следом идут Китай (143,6) и Россия (93,2), отмечается в исследовании.

Больше половины камер в России (почти 8 млн) установлены коммерческими организациями с целью защиты собственности. Около трети (почти 4,5 млн) работают в школах, больницах, правительственных учреждениях и на улицах. Именно эти камеры финансируются из государственного бюджета. Остальные (почти 1,1 млн), по данным исследования, были установлены частными лицами.

Власти многих стран полагают, что камеры видеонаблюдения способствуют снижению преступности, повышают общественную

безопасность и помогают в случае дорожных происшествий. Однако есть серьезные опасения, что они также нарушают частное пространство человека. Более того, ***зачастую неизвестно, где и как хранится эта информация***.

В 2020 г. пандемия коронавируса открыла новую сторону использования камер. Некоторые страны стали применять высокотехнологичное слежение для того, чтобы убедиться, что люди, которых обязали соблюдать карантин, на самом деле оставались дома. Например, в Гонконге ввели в обиход «карантинный браслет», в Южной Корее и России отслеживали перемещения ***по геолокации в телефоне***.

После нескольких лет испытаний Россия ***в январе 2020 г. ввела в строй систему распознавания лиц. Эта технология установлена на более чем 100 тыс. камер в Москве***.

Поэтому к началу пандемии у московских властей уже была ***система, позволяющая отслеживать людей, которые должны были соблюдать карантинные меры***. Людей засекали, даже если они выходили из дома всего на несколько минут выбросить мусор.

В 2020 г. мэрия Москвы выделила на установку системы еще 2,7 млрд руб. Большая часть этих средств — 1,4 млрд руб. — пошла на оснащение ***камерами с системой распознавания лиц для вагонов метро***. В каждом вагоне должно быть по восемь таких камер, но пока это относится только к четверти эксплуатационного парка вагонов. Остальные средства пошли на установку камер в трамваях, электробусах и автобусах, на расширение системы хранения данных и на мобильные комплексы для распознавания лиц на массовых мероприятиях.

Алгоритм искусственного интеллекта распознает лицо, даже если человек использует для маскировки очки, усы или бороду. Уже есть факты, когда распознавались люди в мотоциклетных шлемах, медицинская маска тоже не сработает для защиты от алгоритма.

В июне 2020 г. правительство РФ подписало контракт с Ростехом на установку ***системы распознавания лиц в школах на платформе под названием «Оруэлл»***. Ею планируется охватить более 43 тыс. школ. По заявлению Министерства образования, это делается для того, чтобы мониторить передвижения и действия детей, а также выявлять посторонних в стенах школ.

Дополнительные системы распознавания лиц будут установлены по всей России. Помимо Москвы еще 10 городов будут располагать такими системами в общественных местах и даже у входов в подъ-

езды многоквартирных домов. Например, в Нижнем Новгороде планируют установить около 3000 таких камер.

МВД России разрабатывает систему распознавания людей по татуировкам, по радужной оболочке глаза, по голосу и по движениям тела. Система распознавания по походке способна определить человека на расстоянии 50 метров, даже если он не смотрит в камеру. Она анализирует походку по длине шага, уровню наклона ступни, движению рук, и ее довольно сложно «провести».

Поскольку все технологии слежения в своей основе упираются в базу данных, ***МВД России создает централизованный банк биометрических данных с отпечатками пальцев и изображениями лиц***. В банке данных будет собрана информация как о российских гражданах, так и об иностранцах. Его планируется создать в течение ближайших трех лет.

Следует отметить, что с самого начала установки системы распознавания лиц в Москве начали поступать сообщения об утечках данных.

Протесты, видеонаблюдение, распознание. В ходе следствия, а потом и суда по «болотному делу» о беспорядках на Болотной площади Москвы 6 мая 2012 г. стало понятно, что в основу обвинительных материалов легли записи с камер уличного наблюдения. Новые задержания проводились по мере поступления все новых видеозаписей, эти же кадры использовались в суде как доказательства вины демонстрантов.

Мэрия закупает планшеты и телефоны, с помощью которых сотрудники полиции и чиновники могут вести прямую трансляцию с массовых мероприятий — например, с митингов. Видеопотоки с мобильных камер подключены к ЕЦХД.

С чем сопрягаются данные видеонаблюдения? Естественно, получение самих результатов видеонаблюдения — это только начало углубленной аналитической работы, основанной на технологии Big Data.

Пол, возраст, уровень дохода, социальный статус, номер телефона пассажира в метро уже сейчас можно практически мгновенно узнать благодаря системе персональных коммуникаций.

А всего в распоряжении московской мэрии есть около 170 разнообразных информационных систем. В общей картине люди — лишь часть огромного конгломерата данных, наряду с дорогами, автомобилями, зданиями, канализацией, торговыми палатками, детскими площадками и всем прочим, из чего состоит город. Мэрия наблюдает за всем сразу.

С помощью этих систем можно следить и за любым конкретным человеком.

Частично это обычная официальная информация, которой власти обладали и раньше, просто теперь она переведена в электронные базы данных. ***Данные о браках, разводах и детях хранятся в «едином информационно-телекоммуникационном пространстве» ЗАГС. Все обращения к врачам — в единой медицинской системе. В системе единого расчетного центра (ЕИРЦ), который отвечает за выставление коммунальных квитанций, есть данные о тех, кто зарегистрирован в квартире сейчас, и о тех, кто давно выписался оттуда (так называемые «домовые книги»).***

Но теперь у мэрии есть и данные, которыми раньше она не обладала. Например, огромное количество жителей города живут не по месту официальной регистрации или вовсе без нее. ***Для получения достоверной информации о месте жительства и перемещениях жителей столицы мэрия с 2015 г. закупает геоаналитические данные сотовых операторов.***

По сути, это информация о том, к каким базовым станциям подключались телефоны москвичей и с каким интервалом каждый телефон переходил от одной вышки к другой.

По скорости переподключения абонента от одной вышки к другой понятно, идет он по улице пешком или едет на автомобиле, а по тому, к какой станции телефон чаще всего подключен в ночное время, — где именно человек ночует, а значит, живет.

Операторы передают мэрии данные не напрямую, а через посредника — например, через ***Аналитический центр при правительстве РФ***. В общей сложности с 2015 г. на закупку геоаналитической информации из бюджета Москвы было выделено более 700 млн руб. (включая затраты 2020 г.), следует из информации на сайте госзакупок. За эти деньги мэрия получает так называемые ***«обезличенные» отчеты о количестве абонентов***, проживающих и работающих в разных районах города, с разбивкой по секторам размером 500 × 500 м, а также о том, куда они ходят и ездят каждый день.

Опираясь на данные сотовых операторов, мэрия Москвы предупреждает о закрытии станций всех, кто проживает вокруг них, а не только официально зарегистрированных.

Имея эту информацию, мэрия, к примеру, предупреждает жителей конкретного района о закрытии ближайших к ним станций метро. Такие сообщения от департамента транспорта столицы при-

ходят не только тем, кто зарегистрирован в конкретном районе, но и тем, кто живет в нем без регистрации.

Геоаналитика используется и для ***расчета продовольственной обеспеченности районов***: данные о реальных местах жительства людей накладываются на карту расположения торговых объектов, следует из отчетов Департамента информационных технологий (ДИТ). Кроме того, сотовые данные помогают понять, сколько людей на лето уезжают жить на свои подмосковные дачи, или оценить туристический поток из других регионов России и зарубежных стран (в случае использования роуминга), следует из госконтрактов.

В мэрию отчеты поступают в обезличенном и агрегированном виде — не по каждому отдельному человеку, а сразу по большим группам людей, говорит топ-менеджер data-компании, работавшей со столичным правительством.

Данные о людях можно сегментировать по различным критериям — например, выделить абонентов определенного возраста. Благодаря этому, например, мэрия может видеть, сколько пенсионеров на самом деле соблюдают рекомендованный им режим самоизоляции.

В условиях эпидемии ***мэрия следит и за отдельными людьми*** — например, отправляя сообщения о необходимости самоизоляции пассажирам конкретного рейса. Эта форма контроля осуществляется по другому регламенту и не в рамках контракта на покупку обезличенных агрегированных данных, говорит бывший сотрудник мэрии. Кроме того, в этом случае мэрия уже действует в связке с полицией, у которой больше полномочий такого рода.

Это чрезвычайная ситуация, в рамках нее правительство обязывает операторов совершать определенные действия. Например, по запросам МЧС России они могут отправить жителям конкретного района предупреждение о шторме. По такому же принципу можно действовать, если есть необходимость мониторить определенных людей.

В начале апреля 2020 г. Министерство цифрового развития связи и массовых коммуникаций РФ разработало ***порядок наблюдения за носителями коронавируса на основании данных геолокации сотовых телефонов***, отчасти легализовав тем самым практику, которая сложилась в столице в течение последних нескольких лет.

В особых случаях сотовые операторы и раньше передавали властям данные о местонахождении отдельных людей, вне режима чрезвычайной ситуации и без привлечения полиции. С 2018 г.

действует правило: когда житель Москвы вызывает «скорую» с мобильного телефона, в систему обработки вызовов городской станции скорой помощи поступает информация с точными координатами его местоположения — правда, пока человек все равно должен называть свой адрес оператору скорой.

Информация с сотовых вышек — не единственное «сырье», которое московская мэрия получает от сторонних поставщиков данных.

С момента вступления первых ограничений из-за коронавируса в Москве департамент транспорта ежедневно публикует статистику и аналитику по передвижениям горожан на метро, автобусах и трамваях. В рапорты о том, что все «сидят дома», входит и информация по использованию личных автомобилей, такси и каршеринга.

Как следует из документации на создание элементов интеллектуальной транспортной системы, эти данные чиновники получают напрямую от крупнейших таксомоторных и каршеринговых компаний. Как указано в документах, данные передают «Яндекс. Такси», «Ситимобил», «Везет» и «Gett».

Данные о трафике на московских улицах стекаются в ***Центр организации дорожного движения***.

В Центре организации дорожного движения (ЦОДД подведомствен Дептрансу) подчеркивают: информация о передвижении автомобилей и каршеринга — это треки движения, которые не относятся к персональным данным. ЦОДД получает агрегированные и обобщенные отчеты, сообщили в «Яндекс.Такси» и «Яндекс. Драйве». В «Ситимобиле» и «Везет» добавили, что информация передается в соответствии с двухсторонними соглашениями с мэрией.

Система дает возможность в режиме реального времени отслеживать местонахождение любого такси или взятого напрокат автомобиля, а также узнать всю историю его передвижений. Мэрия также может выгрузить последние фотографии любого транспортного средства, сделанные развешанными по городу камерами фото- и видеофиксации нарушений.

Данные о передвижениях легковых такси и каршеринга в интеллектуальной транспортной системе комбинируются с информацией с датчиков системы ГЛОНАСС, установленных на городском транспорте — автобусах, трамваях и троллейбусах «Мосгортранса», а также на уборочной технике.

Кроме того, например, еще в 2015 г. мэрия договорилась с производителями противоугонных систем о предоставлении данных о передвижении автомобилей по городу.

Система отслеживает и личный автотранспорт, благодаря все той же системе фото- и видеофиксации.

Мэрия имеет доступ к информации о владельцах автомобилей. Совместно с ГИБДД столичное правительство разработало ***систему «Автокод»***, где можно проверить историю регистрации любого транспортного средства и наличие штрафов.

На конец 2018 г. на улицах в пределах Третьего транспортного кольца действовало около 2 тыс. ***Wi-Fi точек***, к которым за год подключились более 665 тыс. человек. Бесплатным интернетом можно воспользоваться в городских парках, библиотеках и музеях. За счет мэрии Wi-Fi получили студенты около 30 московских вузов, причем не только в учебных корпусах, но и в общежитиях.

В 2019 г. столичное правительство решило объединить управление всеми точками в руках одного оператора: конкурс стоимостью 150 млн руб. выиграла ***компания «Максимателеком».*** Она же с 2013 г. обеспечивает работу Wi-Fi в московском метро, но там все устроено иначе: пользователь либо платит за услугу, либо просматривает рекламу перед подключением.

По новому контракту компания не занимается обеспечением доступа в интернет: она должна запустить единое окно авторизации и внутренний портал статистики. С его помощью ***чиновники смогут увидеть, например, с каких телефонов москвичи пользуются Wi-Fi. Более того, оператор вправе использовать технологию DPI для анализа трафика.***

DPI — аббревиатура от англ. ***deep packet inspection, «глубокий анализ пакетов»***. DPI представляет собой программно-аппаратный комплекс, который выделяет в общем потоке трафика конкретные сайты или приложения. Именно DPI российские власти выбрали ***для борьбы с нежелательными ресурсами***, тестирование системы началось в конце 2019 г. Эта же технология поможет чиновникам мэрии понять, какие ресурсы чаще всего посещают москвичи.

Так, отдельно на портале статистики можно посмотреть, какие доли приходятся на шифрованные соединения, торрент-сервисы или просмотр видео. Отдельный раздел посвящен самым популярным у пользователей мессенджерам и топ-100 самых посещаемых ресурсов.

Согласно государственному контракту на портале статистики доступны ***детальные портреты пользователей, составленные на основании того, что именно они делают и ищут в сети***. Каким образом формируются такие портреты?

Вся информация о действиях посетителя на конкретном сайте записывается в ***cookies***. Те, кто имеет доступ к трафику, сопо-

ставляют их друг с другом. Действия, которые с большой вероятностью совершал один и тот же человек, объединяются вместе. Так формируется ***обезличенный профиль пользователя***, рассказывает директор крупной data-компании.

Всех подключавшихся к бесплатному городскому Wi-Fi «Максимателеком» группирует по социально-демографическим признакам — пол, возраст, состав семьи, наличие автомобиля и даже по «жизненным ситуациям», следует из документации.

Портреты могут быть максимально детальными. Вот фрагмент одного из контрактов мэрии на анализ трафика городского Wi-Fi с другой компанией. Для характеристики «имеет автомобиль» аналитики настраивают набор качественных параметров: посещение сайтов парковок, магазинов интернет-запчастей, автосервисов и шиномонтажей; просмотр сайтов удаленных городских объектов (до которых проще добираться на автомобиле).

Еще один источник данных о поведении горожан в интернете — сайт mos.ru и связанные с ним ресурсы вроде «Активного гражданина» или «Нашего города». В 2018 г. общая посещаемость порталов и мобильных приложений семейства mos.ru составила 652 млн визитов (так, через сайт мэрии прошли почти 300 млн обращений за госуслугами). В 2020 г., на фоне эпидемии коронавируса, трафик mos.ru вырос более чем на 50%.

Через собственный трекер мэрия не просто собирает базовую статистику о том, сколько пользователей заходят на городские ресурсы. В отчеты идет информация об IP, стране и браузере пользователя. Следующая задача — ***составить портрет посетителей***.

Система умеет работать даже с теми посетителями mos.ru, которые специально включили режим «инкогнито» в своем браузере, тем самым лишив владельцев сайта возможности собирать cookies. Для этого используется ***технология fingerprint (от англ. «отпечаток пальца»)***, которая является своего рода цифровым аналогом взятия отпечатков пальцев. Только ***вместо рук — уникальные свойства конкретного смартфона, планшета или ноутбука***.

Например, *fingerprint* сообщает часовой пояс устройства, языковые настройки, размер экрана, класс процессора. С помощью нее можно понять, кто приходит к тебе на сайт, даже в том случае, если он использует разные браузеры на своем компьютере.

Собирая детальную информацию, система СТАТС может определять, впервые ли гражданин на mos.ru или уже заходил на него ранее. Если это не первое посещение, система объединяет все сессии вместе и выводит закономерности из действий человека — например, какие услуги ему необходимы или чем он интересуется.

Базовые группы, доступные в системе: одиночные посетители, домохозяйства, схожие социальные группы (например, работники одной компании или представители одинаковых профессий).

Как следует из содержания госконтрактов, внутри этих статистических отчетов могут содержаться и социально-демографические показатели: пол, возраст, доход, семейное положение. Система также умеет находить связь между пользователями внутри группы — например, объединять вместе мужа, жену и детей, если они тоже посещают mos.ru. Мэрия с большой точностью может определить, кто заходит на ее сайты.

Мэрия также собирает ***биометрические данные москвичей — их изображения и образцы голоса***.

Допустим, известны фамилия пассажира и его телефон. Если человек живет в Москве, он не мог не использовать государственные сервисы, и там не могла не сохраниться фотография, пусть и старая. В ход идут не только фото из паспорта, но даже те, которые были сделаны когда-то для льготных проездных школьника или студента.

В случае с заболевшими коронавирусом искать старые фото не нужно: врачей обязали делать фотографии всех находящихся на карантине.

Поиск людей по фотографии-образцу идет внутри всей системы видеонаблюдения, человека можно поставить на контроль, даже если он не проживает по адресу регистрации. Машина, ежедневно обрабатывая изображения москвичей, ранжирует их по принципу «свой — чужой»: тех, кто входит и выходит из одного и того же подъезда постоянно, относит к «своим», новичков — к «чужим».

Пользователь системы может уточнять и детализировать поиск в системе — заставить ее искать человека только среди «своих», только среди «чужих», или искать похожие изображения. Можно указать, за какой период нужны снимки, и даже выставить точность совпадения с образцом — от 50 до 100%.

Системы московской мэрии умеют анализировать и голоса москвичей: с 2015 г. все беседы горожан с сотрудниками единой городской диспетчерской службы не только записываются и затем автоматически расшифровываются в текст, но и оцениваются алгоритмами с точки зрения «эмоционального фона беседы», следует из годового отчета ДИТа.

В 2018 г. подведомственное мэрии АО «Электронная Москва» провело апробацию технологии по автоматическому распознаванию бесед сотрудников сервиса «Мои документы» с посетителями центров госуслуг.

Перед подрядчиком мэрией была поставлена задача — уметь выделять в беседах «стоп-слова», «стоп-фразы» и «слова-конфликтогены», чтобы в дальнейшем автоматизировать оценку качества обслуживания. Согласно контракту система должна записывать все разговоры сотрудников с клиентами, чтобы отслеживать негативные ситуации по ключевым словам.

В этом проекте тестировалась технология компании «Агат-РТ».

В стратегии «Умный город — 2030», принятой в 2018 г., указано: для борьбы с преступностью, помимо системы видеонаблюдения, будут внедрены ***средства «акустического контроля»***. Речь идет о ***чувствительных уличных микрофонах***. Такие устройства уже установлены в ряде городов США и других стран. Их основная задача — распознавать звуки выстрелов, с помощью триангуляции определять их местонахождение и отправлять координаты оператору или ближайшему патрульному экипажу. Они также способны «узнавать» человека по образцу голоса и записывать разговоры: таким образом, с мест совершения преступлений полиция может получать записи не только видео, но и аудио.

Приблизительно в 2015 г. в мэрии пришли к тому, что пора создавать обобщающие системы, которые смогут использовать данные из разных источников. Задача таких систем — не хранить однотипную информацию вроде разрешений на строительство и номеров свидетельств о браке. Они, словно искусственный интеллект из фантастических фильмов, должны отвечать на сложные вопросы и уметь предсказывать будущее.

В Москве разработаны несколько «обобщающих систем», призванных отвечать на вопрос мэра и запросы других чиновников.

Примерно тем же самым занимается известная американская компания ***Palantir***, которая по заказу американских спецслужб переваривает огромный массив данных из разных источников и ищет в них признаки готовящихся преступлений или терактов.

ИАС ДТОИВ умеет аккумулировать и прогонять через себя данные из нескольких источников.

Во-первых, из системы мониторинга криминогенной ситуации, совместной базы данных мэрии и полиции, куда стекается информация обо всех преступлениях и где хранится архивная информация о примерно 5 млн правонарушениях. Данные о штрафах, грабежах и убийствах собираются в ней не только для статистики: система умеет выявлять нетипичную динамику по преступлениям, а также мониторить общественное мнение об уровне безопасности в Москве, в том числе на основании поисковых запросов граждан в интернете.

Во-вторых, из ***«Единого геоинформационного пространства города Москвы»*** — это еще один большой проект мэрии, решившей нанести на электронную карту все городские объекты, в том числе в виде полноценных панорам.

В-третьих, ИАС ДТОИВ подгружает и анализирует данные из СМИ и соцсетей. Раньше для этого использовались ресурсы компании «Медиалогия», но мэрия решила создать свой инструмент для анализа публикаций в интернете — сейчас это часть «системы управления информационными рисками аппарата мэра».

Как ДТОИВ использует весь этот массив данных? Из госконтрактов следует одна из ее задач — предупреждение возможного недовольства жителей новым строительством в своем районе, т.е. выявление потенциальных конфликтов. Одна из задач ИС ДТОИВ — выявлять потенциальные конфликты, связанные с уплотнительной застройкой. Для этого в ДТОИВ есть весь набор данных: программа проводимых слушаний, в том числе по программе реновации, ***сводка по правонарушениям, в том числе связанным с акциями протеста***, и полная выгрузка из медиа и социальных сетей по ключевым словам.

Если ДТОИВ направлена на решение узкопрофильных задач, то ***«система управления данными в распределенной вычислительной среде» (ИС УДРВС)*** может использоваться для очень разных целей — от медицины до анализа интернет-активности горожан.

Она анализирует все данные, содержащиеся в информационных системах и ресурсах мэрии, без их объединения в рамках одной платформы, объясняет руководитель IT-компании, сотрудничающий с ДИТом.

Такая форма более безопасна — ***данные не объединяются в один банк, просто пишется алгоритм, который знает, где их брать***. Система работает по принципу машинного обучения, т.е. сама учится решать поставленную задачу.

Разработка ИС УДРВС началась в 2016 г., а уже в 2018-м она использовалась на практике. Например, ***для выявления «серой аренды» квартир — когда люди сдают свое жилье, но не платят налоги. В официальном отчете ДИТа за 2018 г. этот механизм назван «прогнозированием фактов в отношении аренды»***.

Для поиска «серых» квартир система анализировала информацию о регистрации людей, сотовые данные, данные о парковках, а также просматривала историю коммунальных платежей, платежей за детский сад и другие образовательные услуги, рассказывает бывший сотрудник мэрии.

В ДИТе изучали возможность подписания соглашений с несколькими банками для получения финансовой информации их клиентов, однако в итоге от проекта решили отказаться, говорит экс-сотрудник мэрии. С какими именно банками и почему договориться не удалось, он не уточнил.

Но примерное представление о финансовом положении каждого москвича у мэрии все равно есть. Во-первых, через городские ресурсы идут платежи за ЖКХ и другие госуслуги — более 6,6 млн транзакций на 19 млрд руб. в 2018 г. Во-вторых, власти города знают, какими квартирами и автомобилями владеют (или не владеют) горожане.

Перспективы развития

В правительстве РФ обсуждается разработка ***ГИС «Национальная платформа видеонаблюдения»***, которая объединит в единый контур системы видеонаблюдения, работающие в городах страны. На разработку платформы и установку камер планируется потратить 250 млрд руб. за пять лет. В качестве подрядчика по разработке ГИС рассматривается ООО «Национальные технологии» (49% принадлежит Ростелекому и 51% — Ростеху). Структуры Ростеха займутся аппаратной частью проекта, а Ростелекома — софтверной.

Идея разработки такой ГИС обсуждалась на заседании межведомственной комиссии по внедрению и развитию аппаратно-программного комплекса (АПК) технических средств «Безопасный город» (в нее входят МЧС, Минпромторг, МВД, ФСБ) 13 мая 2021 г.

Предполагается, что ГИС «Национальная платформа видеонаблюдения» станет составной частью обновленного АПК «Безопасный город».

Весь проект оценивался ранее в 97 млрд руб. Источником финансирования может стать госкорпорация «ВЭБ.РФ», которая в рамках концессионных соглашений либо контрактов жизненного цикла выделит каждому субъекту Федерации до 3 млрд руб. на закупку решений для АПК.

Проект «Национальная платформа видеонаблюдения» предполагает масштабирование технологии, которая применяется в Москве, но с другим подходом, объясняет источник, близкий к проекту. Сейчас городские системы видеонаблюдения отправляют видео в ЦОД методом непрерывного потока. Но многие эксперты считают, что это тупиковая технология, которая требует слишком

большого числа ЦОД, поэтому камеры, которые запустят в рамках ГИС, планируется оснащать вычислительными модулями.

Благодаря этому камера будет самостоятельно распознавать и фиксировать преступления и только после этого отправлять видеопоток в ЦОД.

Встроенная нейросеть может давать оценку происходящему в кадре, а встроенное в камеру хранилище позволяет вести непрерывную запись, но с ограничениями по периоду наблюдения.

Отдельные производители камер предлагают функцию распознавания номеров и даже лиц. Камеры со встроенной аналитикой и возможностью записи уже активно используются в ритейле и промышленности.

Хотя техническая возможность перехода к анализу данных на камерах, а не в ЦОД уже существует, это не означает, что тотальный переход на новую технологию будет экономически оправдан. «Умная» камера дороже обычной в 2–6 раз. Помимо этого при ретроспективном анализе событий часто нужен весь контент за определенный период, а не только фрагменты.

Вопрос целесообразности установки камер с вычислительными модулями будет решаться в зависимости от конкретных задач. В одной точке города понадобится быстро фиксировать инциденты и распознавать лица — там будут стоять камеры с мощными вычислительными модулями, а в другой точке могут поставить более дешевые — только с датчиком движения.

Видео в цвете

Серьезной проблемой систем видеонаблюдения долгое время было качество изображения в темное время суток, что играло на руку преступникам. Ведь две трети убийств, разбоев и грабежей происходят ночью. При недостаточном освещении детализация видеоизображения снижается. Кроме того, большинство видеокамер автоматически переключаются в черно-белый формат (ночной режим).

Традиционно в такой ситуации применяется инфракрасная подсветка: при уровне освещенности ниже порогового значения ИК-фильтр убирается, а излучение ИК-подсветки, отраженное от объектов, на которые направлены видеокамеры, формирует черно-белое изображение. При использовании ИК-подсветки разглядеть подробности происходящего перед видеокамерой можно, однако понять, какого цвета детали, уже не получится. Это ограничивает возможности по обеспечению безопасности и идентификации лиц, подозреваемых в преступлении.

Чтобы решить проблему повышения светочувствительности систем видеонаблюдения, совместить четкое изображение и яркие детали, компания *Dahua Technology* разработала технологию *Full-color*.

Современные модели Dahua Full-Color оснащены светодиодной подсветкой, которая имеет теплый спектр, поскольку желто-зеленые цвета более безопасны для зрения человека. Здесь применяется излучение с температурой 3000 К, что соответствует европейскому стандарту EN62471, который оценивает степень вреда для глаз различных источников света.

Среди других ключевых составляющих технологии Full-color — матрица Ultra Starlight, объектив с большой диафрагмой, алгоритм шумоподавления 4.0.

В Full-color от Dahua Technology используются высокочувствительные матрицы Ultra Starlight. Высокую эффективность и рост светочувствительности на 30% обеспечивает увеличение физического размера матрицы. Для Ultra Starlight характерен больший, чем обычно, размер пикселя, что позволяет получить больше света за время накопления заряда. Кроме того, технология Full-color имеет высокий коэффициент преобразования падающего света и обратную засветку пикселей. Поскольку фотодиоды оказались над металлической проводкой, она больше не блокирует поток света, что увеличивает светочувствительность матрицы.

Объектив с большой диафрагмой F1.0 в видеокамерах Full-color пропускает в 2,5 раз больше света по сравнению с F1.6, что значительно повышает эффективность при низких уровнях освещенности. Чем больше света, тем ярче изображение. В объективах установлены специальные асферические гибридные линзы, при производстве которых используется и стекло, и пластик. Результат — улучшенная коррекция оптических искажений, снижение веса и размера изделия.

Для подавления шумов в видеокамерах с технологией Full-color используется собственная разработка Dahua — новейший ISP-процессор четвертой версии. Обработка двухмерной и трехмерной информации позволяет улучшить соотношение сигнал/шум и цветопередачу. В итоге ночью передается четкое цветное изображение не только статичных, но и движущихся объектов.

Оператор круглосуточно получает цветное изображение с более яркими и четкими деталями даже ночью. Наряду с этим:

— видеокамеры данного типа могут использоваться в качестве дополнительного освещения;

— возможен поиск по цвету объекта в видеозаписях, полученных в условиях низкой освещенности;

— технология Full-color за счет большей детализации в видимом спектре позволяет улучшить распознавание лиц минимум на 15% по сравнению с обычной видеокамерой с ИК-подсветкой;

— обнаружение объектов на значительно большем расстоянии обеспечивают вышеупомянутый объектив с большой диафрагмой F1.0 и высокочувствительная матрица;

— в видеокамерах Full-color без подсветки отсутствует отражение подсветки от дождя; кроме того, она не привлекает насекомых, что сказывается на качестве передаваемого изображения.

Dahua Technology разработала линейку TiOC (Three-in-One Camera) на основе инновационных видеокамер, в которых *технология Full-color сочетается с алгоритмами ИИ и функцией активного сдерживания*. Это интегрированное решение «три в одном» позволяет значительно экономить время и средства при установке, объединяя такие функции, как круглосуточное видеонаблюдение в цвете, система оповещения с функцией активного сдерживания и возможности ИИ.

Международно-правовое регулирование защиты данных, полученных в ходе видеонаблюдения

28 января 1981 г., 40 лет назад, в Страсбурге был открыт для подписания первый имеющий обязательную силу международный договор, удовлетворяющий потребность в защите персональных данных, — ***Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных***, также известная как «Конвенция 108» (ратифицирована в России Федеральным законом от 19 декабря 2005 г. № 160-ФЗ, вступила в силу для нее 1 сентября 2013 г.). Договор был модернизирован в 2018 г. путем принятия Протокола о внесении изменений, который еще не вступил в силу. Протокол направлен на обеспечение того, чтобы принципы защиты персональных данных были адаптированы к новым технологиям, а также на укрепление предусмотренного Конвенцией контрольного механизма.

В 1981 г. «Конвенция 108», открытая для всех стран и обладающая уникальным потенциалом стать глобальным стандартом, закрепила основополагающие принципы и правила защиты данных, которые применяются и сегодня. Конвенция, составленная в нейтральном стиле с точки зрения технологий, полностью сохраняла свою актуальность на протяжении четырех десятилетий. На сегодняшний день она насчитывает 55 стран-участниц на четырех

континентах, еще 20 государств принимают участие в ее работе. Во многих государствах по всему миру «Конвенция 108» стала базой соответствующего национального законодательства. Кроме того, она послужила основой для первой директивы Европейского союза по защите данных, принятой в 1995 г., за которой в 2018 г. последовало принятие «Общего регламента по защите данных» (GDPR).

Одной из целей Протокола 2018 г., модернизирующего Конвенцию, являются сведение воедино различных нормативных рамок, разработанных в разных регионах мира, в том числе в Европейском союзе, и предоставление гибкого, прозрачного и надежного многостороннего инструмента, призванного содействовать трансграничной передаче потока данных, обеспечивая эффективные гарантии от злоупотреблений, связанных с данными. Десять государств уже ратифицировали и 33 государства подписали Протокол, создающий эту модернизированную «Конвенцию 108+». Совет Европы порекомендовал строгие правила, чтобы избежать значительных рисков для неприкосновенности частной жизни и защиты персональных данных, которые связаны с растущим использованием технологий распознавания лиц. Кроме того, некоторые приложения для распознавания лиц должны быть полностью запрещены, чтобы избежать дискриминации.

В январе 2021 г. приняты ***новые Руководящие принципы по распознаванию лиц***, адресованные правительствам, законодателям и руководителям предприятий, правозащитным организациям. Руководящие принципы были разработаны Консультативным комитетом по Конвенции о защите физических лиц при автоматизированной обработке персональных данных, который объединяет экспертов, представляющих 55 государств — участников Конвенции, а также 20 стран-наблюдателей.

Руководящие принципы предлагают ***запретить использование распознавания лиц, если это продиктовано лишь целью определения цвета кожи, религиозных или иных убеждений, пола, расового или этнического происхождения, возраста, состояния здоровья или социального статуса человека.***

Запрет должен распространяться и на так называемые технологии распознавания эмоций, позволяющие по выражению лица определять личностные качества, внутренние ощущения, психическое состояние или уровень вовлеченности сотрудников в работу, поскольку эти технологии сопряжены с серьезными рисками в таких областях, как трудоустройство, доступ к страхованию и образованию.

В соответствии с новыми Руководящими принципами при использовании технологий распознавания лиц в ***государственном секторе*** согласие, как правило, не должно быть правовым основанием, используемым для распознавания лиц государственными органами, учитывая дисбаланс полномочий между субъектами данных и государственными органами. По той же причине, как правило, это не должно быть правовым основанием для распознавания лиц, выполняемого ***частными лицами, уполномоченными решать задачи, аналогичные задачам государственных органов***.

Законность использования технологий распознавания лиц должна основываться на целях биометрической обработки, предусмотренных законом, и необходимых гарантиях, дополняющих Конвенцию 108+.

Законодатели и лица, принимающие решения, должны установить конкретные правила обработки биометрических данных с помощью технологий распознавания лиц в правоохранительных целях. Эти законы будут гарантировать, что такое использование должно быть строго необходимым и соразмерным данным целям, и предписывать необходимые меры безопасности.

Обработка биометрических данных с помощью технологий распознавания лиц для целей идентификации в контролируемой или неконтролируемой среде, как правило, ограничивается целями правоохранительных органов. Она должна выполняться исключительно компетентными органами в области безопасности. Законы могут предусматривать различные тесты на необходимость и соразмерность в зависимости от того, является ли цель проверкой или идентификацией, с учетом потенциальных рисков для основных прав и при условии, что изображения людей собираются на законных основаниях.

Для целей идентификации должны соблюдаться строгая необходимость и соразмерность как при создании базы данных (список наблюдения), так и при развертывании (в реальном времени) технологий распознавания лиц в неконтролируемой среде. Законы должны предусматривать четкие параметры и критерии, которым должны следовать правоохранительные органы при создании баз данных (списков наблюдения) для конкретных, законных и явных правоохранительных целей (например, подозрение на серьезные правонарушения или риск для общественной безопасности).

На этапе развертывания технологий распознавания лиц в режиме реального времени в неконтролируемых средах закон должен гарантировать, что правоохранительные органы продемонстрируют, что множество факторов, включая место и время развертывания

этих технологий, оправдывают строгую необходимость и пропорциональность использования.

Понятие «контролируемая среда» охватывает случаи, когда биометрические системы могут использоваться только с участием человека.

Законодатели и лица, принимающие решения, должны гарантировать, что ясная и точная правовая основа обеспечивает необходимые гарантии для обработки биометрических данных. Такая правовая основа будет включать строгую необходимость и соразмерность такого использования и будет учитывать ***уязвимость субъектов данных и характер среды, в которой эти технологии используются для целей проверки***.

Использование технологий распознавания лиц ***частными организациями***, за исключением частных лиц, уполномоченных выполнять задачи, аналогичные задачам государственных органов, требует в соответствии со ст. 5 Конвенции 108+ явного, ***конкретного, бесплатного и информированного согласия субъектов, биометрические данные которых обрабатываются***.

С учетом требования о таком согласии субъектов данных использование технологий распознавания лиц может иметь место только в контролируемых средах для проверки, аутентификации или категоризации. В зависимости от цели особое внимание следует уделять качеству явного согласия субъекта данных, когда оно является правовой основой для обработки.

Чтобы гарантировать, что согласие дано свободно, субъектам данных должны быть предложены ***решения, альтернативные технологии распознавания лиц*** (например, с применением пароля или идентификационного бейджа), которые просты в использовании.

Если согласие дано для определенной цели, личные данные не должны обрабатываться способом, несовместимым с этой целью. В случае раскрытия данных третьей стороне такое раскрытие также должно быть предметом специального согласия.

Частные организации не должны использовать технологии распознавания лиц в неконтролируемых средах, таких как торговые центры, особенно для идентификации лиц, представляющих интерес, в маркетинговых целях или в целях частной безопасности. Прохождение через среду, в которой используются технологии распознавания лиц, не может рассматриваться как явное согласие.

В соответствии со ст. 15 (3) Конвенции 108+ ***надзорные органы*** должны консультироваться по предложениям о любых законода-

тельных или административных мерах, предполагающих обработку персональных данных с помощью технологий распознавания лиц. Необходимо систематически привлекать контролирующие органы и, в частности, консультироваться с ними по поводу любых возможных экспериментов или предполагаемого развертывания. Таким образом, с этими органами должны проводиться систематические консультации до запланированных проектов. Кроме того, они должны иметь доступ к проведенным оценкам воздействия, а также ко всем отчетам, документам по аудитам и анализу, проведенным в контексте таких экспериментов или проектов.

Законодатели и лица, принимающие решения, должны обеспечить эффективное сотрудничество между различными органами, компетентными в надзоре за отдельными аспектами обработки данных, когда разные органы несут ответственность за контроль соответствия такой обработки данных закону.

Определенные законодателем меры безопасности должны развиваться с течением времени и в ответ на меняющиеся угрозы и выявленные уязвимости. ***Они должны быть пропорциональны чувствительности данных, контексту, в котором используется конкретная технология распознавания лиц, и ее целям, вероятности причинения вреда отдельным лицам и другим соответствующим факторам. Строгие методы хранения и утилизации — с помощью безопасных процедур — данных распознавания лиц с минимально возможными сроками хранения также способствуют снижению рисков безопасности.***

Законодательные органы и лица, принимающие решения, должны использовать различные механизмы для обеспечения подотчетности разработчиков, производителей, поставщиков услуг или организаций, использующих эти технологии. Создание независимого и квалифицированного ***механизма сертификации*** для распознавания лиц и защиты данных, с тем чтобы продемонстрировать полное соответствие выполняемых операций обработки требованиям, могло бы стать важным элементом в укреплении доверия пользователей. Такая сертификация может быть реализована в соответствии ***с применением искусственного интеллекта, используемого технологией распознавания лиц: один тип сертификации для категоризации структур (разработка алгоритма, интеграция алгоритма и т.д.), а другой — для категоризации алгоритмов (компьютерное распознавание, интеллектуальный поиск и т.д.).***

Осведомленность субъектов данных и понимание широкой общественностью технологий распознавания лиц и их влияния

на основные права должны активно поддерживаться доступными средствами и образовательными мероприятиями.

Идея состоит в том, чтобы предоставить доступ к простым концепциям, которые могли бы предупредить субъектов данных до того, как они решат использовать технологию распознавания лиц, чтобы они понимали, что значит использовать конфиденциальную информацию, такую как биометрические данные, как работает распознавание лиц, и предупредить их о потенциальной опасности, особенно в случае неправильного использования. Законодательные органы и лица, принимающие решения, должны способствовать участию общественности в разработке и использовании этих технологий и в обеспечении надлежащих гарантий для защиты основных прав, поставленных на карту при использовании распознавания лиц.

Помимо проблем, изложенных в новых Руководящих принципах, важно учитывать и мировой опыт. Например, в Великобритании с 2012 г. действует строгое законодательство, регулирующее работу с камерами уличного наблюдения, а также хранение и доступ к информации.

Кодекс применения камер наблюдения создан, по замыслу авторов, для того, чтобы соблюсти баланс между необходимостью вести наблюдение и невмешательством в частную жизнь.

Для России крайне актуальна борьба с «утечками» персональных данных из государственных и частных банков информации: ***данные из некоторых систем можно купить на так называемом рынке «пробива»***.

«Пробивом» на жаргоне называется покупка персональных данных, в основном на специализированных форумах в интернете с простой системой регистрации. Для покупки доступна информация из баз сотовых операторов, банков, МВД России, ФНС России и прочих государственных органов. Можно встретить предложения купить данные о парковочных сессиях, выписку из ЗАГСа или домовой книги, а также записи с любой видеокамеры.

Более 6,3 тыс. камер видеонаблюдения, размещенных в том числе на объектах критической инфраструктуры и промышленных предприятиях России, имеют ***открытые IP-адреса, а доступ к ним может получить любой желающий***. На базе камер с открытым IP злоумышленники могут организовать нелегальную систему видеонаблюдения или использовать их как вычислительный ресурс, предупреждают эксперты.

Порядка 6,3 тыс. камер видеонаблюдения, расположенных на электростанциях, промышленных предприятиях, заправках

и в системах «умных» домов в России, оказались уязвимы. IP-адреса этих камер открыты, и к ним могут получить доступ хакеры.

К системе большинства таких камер можно получить доступ без имени пользователя и пароля, либо пароль к ним установлен по умолчанию.

Россия, по данным *Shodan.io*, находится на пятом месте по числу камер видеонаблюдения с открытым IP. На первых строчках располагаются Вьетнам, Тайвань, Южная Корея и США. Во всем мире около 124 тыс. камер имеют такую уязвимость.

В сентябре 2020 г. общественная организация «Роскомсвобода» в суде потребовала от властей Москвы остановить работу уличной системы по распознаванию лиц. Организация была обеспокоена тем, что в даркнете можно легко купить подробные данные о передвижениях людей, которые собираются с помощью городских камер. В январе 2021 г. пользователь сайта Habr обнаружил уязвимость, позволяющую проникнуть в систему видеонаблюдения ОАО «РЖД». Проблема была связана с незамененными паролями, установленными по умолчанию на маршрутизаторах компании «MikroTik».

Доступ к ряду камер сегодня защищен самыми простыми паролями, которые легко подобрать. Такие камеры могут быть размещены в том числе в банках, что грозит утечками данных пластиковых карт и паспортов клиентов кредитных организаций. На базе камер с открытым IP можно организовать нелегальную систему видеонаблюдения или аналитики. Если дополнить такую систему модулями распознавания лиц, получится система слежки.

Злоумышленники могут, например, зайти в корпоративную сеть компании через уязвимые камеры, создать сеть ботов или использовать их как вычислительный ресурс.

Если уязвимые камеры видеонаблюдения установлены дома, то их взлом грозит нарушением тайны частной жизни.

Дальнейшее развитие технологий

«Ntechlab» (технологический партнер Ростеха) разработал систему ***распознавания лиц***, которая уже применяется в ряде регионов РФ. Теперь компания объединила ее с функцией ***распознавания силуэтов людей и машин***. Компания представила платформу ***мультиобъектной видеоаналитики***, которая в режиме реального времени отображает видеопотоки, распознавая силуэты прохожих и автомобилей. Система распознавания лиц и силуэтов применяется МВД России в пяти регионах РФ.

Алгоритм при распознавании внешне похожих людей будет учитывать такие признаки, как походка, рост и т.д., а также позволит осуществлять поиск по таким атрибутам внешности, как, например, очки, шляпа или борода.

То же и с автомобилями. Все уже привыкли к тому, что автомобили регистрируются дорожными камерами, но таких камер не так много и они делают снимки только на городских дорогах, хайвеях. Рассматриваемая система умеет распознавать автомобили и с тех камер, с которых они не очень хорошо видны — когда нельзя распознать номера или видна только часть автомобиля. Алгоритм позволяет идентифицировать автомобиль, определяя его цвет, марку, индивидуальные особенности.

* * *

Учитывая остроту восприятия в общественном сознании проблем, связанных с видеонаблюдением и персональными данными в целом, процессом распознавания и использования полученных результатов в правоприменительной и судебной деятельности, следует адаптировать международно-правовые требования и рекомендации по нормативному регулированию этих вопросов для российских государственных органов и частных компаний.

Возможно, потребуется и внесение изменений в российское законодательство, в том числе в Уголовно-процессуальный кодекс РФ и в ФЗ об ОРД.

Кроме того, необходима ведомственная регламентация использования видеонаблюдения в ОРД.

А.А. Маслов

Оперативно-розыскное обеспечение коллективной безопасности в условиях информационного общества

За последние годы в России принят целый ряд документов стратегического планирования, регламентирующих вопросы развития информационного общества и цифровой экономики, обеспечения информационной безопасности, в том числе безопасности критической информационной инфраструктуры, а также использования современных ИКТ в различных сферах жизнедеятельности российского общества[1].

Благодаря своевременному их принятию и реализации в настоящее время возможно решать значительное количество социально-экономических проблем, в том числе достаточно эффективно противостоять вызовам и угрозам, возникшим вследствие продолжающейся пандемии коронавируса.

При этом пандемия проявила себя в основном как катализатор тенденций, которые начали входить в нашу жизнь в конце 10-х гг. нового тысячелетия, — это дистанционные форматы общения, развитие электронно-цифровых сервисов, телекоммуникационных и мобильных сетей, применение методик обработки «больших данных», «облачных» вычислений, внедрение технологий ИИ, интеграция современных технологий в финансовый сектор[2].

Активное формирование информационного общества, а также национального и транснационального информационного пространства создает новые условия для деятельности органов, осуществляющих ОРД в целях защиты личности, общества и государства от преступных посягательств, которые являются предметом иссле-

[1] Указы Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы», от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» и т.д.

[2] *Кудрин А.Л.* Вступительная статья // *Жданов Ю.Н., Кузнецов С.К., Овчинский В.С.* COVID-19: преступность, кибербезопасность, общество, полиция. М.: Международные отношения, 2020. С. 7.

дования и осмысления для специалистов в сфере борьбы с преступностью. Так, справедливо отмечается, что отличительной чертой нашего времени является окончательное стирание границ и различий между реальностью и виртуальностью, между миром вещей и миром информации, между деятельностью онлайн и офлайн, между социальной средой и киберсредой[1].

Новые условия деятельности оперативных подразделений полиции связаны с тем, что в современном мире не осталось ни одной сферы человеческой деятельности, в которую цифровые технологии не привнесли бы кардинальных изменений, что, с одной стороны, создает дополнительные возможности в повышении эффективности их деятельности. То, что еще вчера казалось фантастикой, даже не научной, оказывается в наши дни вполне рабочим инструментом (например, чтение мыслей, распознавание речи на расстоянии по движению лица, наконец, предсказание поведения человека)[2].

С другой стороны, активная деятельность представителей криминалитета в цифровой среде, высокий уровень его организованности и технологичности уже породили существенные проблемы нового качества в оперативно-розыскном противодействии преступности.

При этом следует отметить, что *киберпреступность является единственным, но очень наглядным, проявлением трансграничности и масштабности современных вызовов и угроз правам и свободам миллионов граждан, безопасности общества и государства.*

По прогнозу Всемирного экономического форума, к 2022 г. сумма планетарного материального ущерба от кибератак будет только возрастать и составит около 8 трлн долл.[3] По этой причине эффективное противодействие преступлениям, совершаемым с использованием ИКТ, невозможно без совершенствования действующих и создания новых механизмов международного сотрудничества, а также принятия соответствующих правовых мер по укреплению коллективной безопасности государств.

---

1 *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. М.: Международные отношения, 2020. С. 16.

2 *Шаронов А.* Полиция будущего — это технологии будущего // *Жданов Ю., Овчинский В.* Полиция будущего. М., 2018. С. 4.

3 *Кузнецов С.К.* Киберпреступность и киберполиция не имеют национальных границ // *Жданов Ю.Н., Овчинский В.С.* Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. М.: Международные отношения, 2020. С. 9.

Вместе с тем конец XX и начало XXI в. ознаменованы появлением иных не менее опасных для жизни, здоровья, прав и свобод личности, стабильности общества и суверенитета государства вызовов и угроз, связанных с терроризмом, экстремизмом, незаконным оборотом наркотиков и оружия, коррупцией, торговлей людьми и пр., каждая из которых в отдельности и все они в совокупности требуют принятия коллективных мер реагирования, которые немыслимы без активного задействования возможностей и ресурсов ОРД.

В связи с этим *в современных условиях развития информационного общества формирование системы оперативно-розыскного обеспечения коллективной безопасности России и ее союзников является одной из наиболее актуальных проблем теории и практики ОРД.*

Ретроспективный анализ показывает, что проблема обеспечения коллективной безопасности имеет давнюю историю. Так, во времена Советского Союза активно действовало военно-политическое объединение — Варшавский договор, которое носило оборонительный характер и противостояло блоку НАТО, обеспечивая, в первую очередь военными силами и средствами, безопасность и территориальную целостность государств-участников.

Прошло уже более четверти века, как не стало данной организации. К сожалению, на сегодняшний день мы можем констатировать, что международная система безопасности из-за этого понесла невосполнимый урон, в результате чего мир стал фактически однополярным и, как следствие, более конфликтным.

Современный анализ международного противоборства показывает, что тактика действий внешних враждебных сил такова, что в условиях гибридных войн и оранжевых революций делаются постоянные попытки целенаправленно усилить и деструктивно использовать именно внутренние вызовы и угрозы национальной безопасности Российской Федерации и ее союзников, которые непосредственно связаны с жизнью и благополучием сотен миллионов граждан.

Данное обстоятельство во взаимосвязи со стремительным ростом преступлений, совершаемых с использованием ИТТ, позволяет сделать вывод об объективной необходимости усиления роли ОРД как гласной и негласной деятельности правоохранительных органов в обеих сферах (*реальной и виртуальной*), *и расширения содержания коллективной безопасности за счет развития организации и тактики противодействия этим угрозам с использованием ее сил, средств и методов.*

Такие наиболее опасные социальные явления, как экстремизм, терроризм, организованная преступность, незаконный оборот наркотиков и оружия, нелегальная миграция, киберпреступления, т.е. то, что Стратегией национальной безопасности Российской Федерации[1] отнесено к наиболее опасным вызовам и угрозам, в условиях использования новых ИКТ приобрели транснациональный характер, следовательно, противодействие им требует принятия комплексных мер, в том числе на международном уровне.

Противодействие преступлениям международного характера входит в уставные задачи различных международных организаций, участницей которых является Российская Федерация.

В рамках данной статьи вопросы оперативно-розыскного обеспечения коллективной безопасности предполагается рассмотреть на примере Организации Договора о коллективной безопасности (ОДКБ), участниками которой на сегодняшний день являются Россия, Армения, Белоруссия, Казахстан, Киргизия и Таджикистан.

В ст. 8 Устава данной Организации от 7 октября 2002 г. указано, что государства — члены ОДКБ координируют и объединяют свои усилия в борьбе с международным терроризмом и экстремизмом, незаконным оборотом наркотических средств и психотропных веществ, оружия, организованной транснациональной преступностью, нелегальной миграцией и другими угрозами безопасности государств-членов. При этом данные государства:

1) принимают меры к созданию и функционированию в рамках ОДКБ системы реагирования на кризисные ситуации, угрожающие безопасности, стабильности, территориальной целостности и суверенитету государств-членов;

2) взаимодействуют в сферах охраны государственных границ, обмена информацией, информационной безопасности, защиты населения и территорий от чрезвычайных ситуаций природного и техногенного характера, а также от опасностей, возникающих при ведении или вследствие военных действий;

3) осуществляют свою деятельность на этих направлениях, в том числе в тесном сотрудничестве со всеми заинтересованными государствами и международными организациями при главенствующей роли ООН.

14 октября 2016 г. решением Совета коллективной безопасности данной Организации утверждена Стратегия коллективной безопасности ОДКБ на период до 2025 года (далее — Стратегия), которая

[1] Указ Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

определила стратегические цели, задачи и основные направления развития ее системы.

В Стратегии также приведены определения основных понятий, используемых в данной сфере. Так, *коллективная безопасность — это состояние защищенности коллективных интересов государств — членов ОДКБ, которое позволяет обеспечить независимость, территориальную целостность, суверенитет, обороноспособность и защиту от угроз каждому из государств — членов ОДКБ на основе координации и осуществления совместной деятельности.*

Кроме того, в Стратегии определены такие понятия, как зона ответственности ОДКБ, вызов коллективной безопасности ОДКБ, угроза коллективной безопасности ОДКБ, система коллективной безопасности ОДКБ, силы и средства коллективной безопасности ОДКБ и т.д.

Все это создает условия для разработки на примере ОДКБ организационно-правовых основ оперативно-розыскного обеспечения коллективной безопасности, которые будут актуальны для различных форматов коллективной безопасности, как многосторонних, так и двухсторонних.

Формируемая правовая основа в рамках ОДКБ регламентирует деятельность Организации по всем направлениям обеспечения безопасности, включая правоохранительные аспекты. К настоящему моменту подписано 48 межгосударственных соглашений и 227 решений Совета коллективной безопасности[1].

Стратегической целью ОДКБ является обеспечение коллективной безопасности путем консолидации усилий и ресурсов государств-членов на основе стратегического партнерства и общепризнанных норм и принципов международного права.

---

[1] См.: Соглашение о взаимном обеспечении сохранности секретной информации в рамках ОДКБ (Астана, 18 июня 2004 г.); Соглашение о льготных условиях поставок специальной техники и специальных средств для оснащения правоохранительных органов и специальных служб государств — членов ОДКБ (Душанбе, 6 октября 2007 г.); Соглашение о сотрудничестве государств — членов ОДКБ в области обеспечения информационной безопасности (Минск, 30 ноября 2017 г.); Решение Совета коллективной безопасности ОДКБ «Об Антинаркотической стратегии государств — членов ОДКБ на 2015–2020 годы» (Москва, 23 декабря 2014 г.); Решение Совета коллективной безопасности ОДКБ «О Положении о формировании Единого списка организаций, признанных террористическими в формате ОДКБ» (Ереван, 14 октября 2016 г.); Решение Совета коллективной безопасности ОДКБ «О совершенствовании мер по противодействию незаконной миграции» (Минск, 30 ноября 2017 г.) и др.

В основе рассматриваемой системы лежит принцип обеспечения коллективной безопасности через укрепление национальной безопасности каждого государства — члена ОДКБ, которое в части противодействия транснациональным вызовам и угрозам невозможно без полноценного оперативно-розыскного обеспечения.

Во всех государствах — членах ОДКБ приняты законы, регулирующие ОРД[1], в которых закреплены ее цели, задачи, принципы, основания и условия проведения оперативно-розыскных мероприятий (ОРМ) и иные значимые вопросы. Сравнительно-правовой анализ показывает, что, несмотря на имеющиеся различия в регламентации частных вопросов, все законодательные акты концептуально схожи между собой. Однако это не исключает проявления самобытности законодателя, демонстрации им собственного подхода к положениям, касающимся содержания ОРД, перечня ОРМ, их определений, организации использования негласной помощи граждан и т.д.

При этом продолжается процесс совершенствования данных законов. Так, в относительно недавно принятом Законе Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» достаточно подробно регламентированы права и обязанности субъектов оперативно-розыскных отношений. Кроме того, данный Закон содержит пример разрешения имеющей давнюю историю проблемы допуска конфидентов к сведениям, составляющим государственные секреты (тайну).

Процесс совершенствования национальных законодательств в сфере ОРД государств — членов ОДКБ создает благоприятные условия для поэтапного формирования правовой основы оперативно-розыскного обеспечения коллективной безопасности. Вместе с тем нельзя не учитывать потенциальную опасность утраты или ослабления общего правового пространства в случае несбалансированного изменения национальных законов в той или иной области.

В связи с изложенным *важно, чтобы первый этап формирования правовых основ оперативно-розыскного обеспечения коллективной*

[1] См.: Закон Республики Армения от 19 ноября 2007 г. № ЗР-223 «Об оперативно-розыскной деятельности»; Закон Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности»; Закон Республики Казахстан от 15 сентября 1994 г. № 154-XIII «Об оперативно-розыскной деятельности»; Закон Киргизской Республики от 16 октября 1998 г. № 131 «Об оперативно-розыскной деятельности»; Федеральный закон от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности»; Закон Республики Таджикистан от 25 марта 2011 г. № 68 «Об оперативно-розыскной деятельности».

безопасности был связан с разработкой мер по сближению и гармонизации оперативно-розыскных законов государств — членов ОДКБ[1].

Такие меры должны предусматривать укрепление и расширение межгосударственного пространства правового регулирования ОРД, в рамках которого всеми участниками признаются общие цели, задачи и принципы данной деятельности, развиваются предиктивная (превентивная) и разведывательно-поисковая функции ОРД, формируется правовая основа общего (скоординированного либо совместного) оперативно-розыскного обеспечения коллективной безопасности.

В соответствии с установленными процедурами автором данной статьи в соавторстве с А.А. Бабушкиным были разработаны Рекомендации по сближению и гармонизации законов государств — членов ОДКБ об оперативно-розыскной деятельности[2] (далее — Рекомендации), которые приняты 26 октября 2015 г. на VIII заседании Парламентской Ассамблеи. Этому предшествовала рассылка проекта во все правоохранительные органы государств — членов ОДКБ для изучения и дачи заключения.

В Рекомендациях конкретизируется для использования в национальных оперативно-розыскных законах понятие ОРД, которое должно более полно отражать ее содержание, особенно в контексте международного (межгосударственного) сотрудничества.

Так, *оперативно-розыскная деятельность* определена как *научно обоснованная система установленных настоящим Законом гласных и негласных оперативно-розыскных мероприятий и действий уполномоченных государственных органов, осуществляемых в соответствии с законодательством о государственной тайне в целях защиты жизни, здоровья, прав и свобод человека и гражданина, собственности, обеспечения безопасности общества и государства от преступных посягательств.*

Практика показывает, что кроме подготовки и проведения ОРМ содержание ОРД составляют и иные законные действия в сфере агентурной работы, информационно-аналитического обеспечения, оперативно-розыскного документирования и т.д. Они могут быть самостоятельным предметом международно-правового регулиро-

---

[1] См.: *Кудачкин А.* Сближение и гармонизация законодательств: понятие и международно-правовая характеристика // Право и жизнь: независимый правовой журнал. 2006. № 99. С. 17–23.

[2] Справочно: разработчиками Рекомендаций применялось написание термина «оперативно-розыскная деятельность» и всех производных от него словосочетаний через «О» в соответствии с названиями законов об ОРД государств — членов ОДКБ.

вания. Данный аспект обозначен в Законе Республики Казахстан и достаточно подробно раскрыт в специальной литературе[1].

В предлагаемом определении ОРД гласная форма проведения ОРМ увязана с законодательством о государственной тайне, согласно которому результаты таких мероприятий не всегда подлежат разглашению. Межгосударственное сотрудничество в сфере ОРД в нынешних условиях не может развиваться без укрепления принципа конспирации.

Кроме того, в Рекомендациях предлагаются нормы, направленные на укрепление предиктивных (предупредительных) возможностей ОРД за счет введения оснований для проведения полного комплекса ОРМ в отношении лиц, находящихся под административным надзором, условно осужденных и условно-досрочно освобожденных.

Рекомендуемая норма изложена следующим образом:

«*Основаниями для проведения оперативно-розыскных мероприятий являются наличие*: *возбужденного уголовного дела*; *судебного решения об установлении в отношении лица административного надзора*, *на весь период его осуществления*; *судебного решения в отношении лица об условно-досрочном освобождении*, *на период неотбытой части наказания*; *судебного решения в отношении лица об условном осуждении*, *на период испытательного срока*».

Так, в Российской Федерации в 2020 г. под административным надзором состояло более 116 120 ранее судимых лиц, из которых 54 463 совершили преступления при опасном и особо опасном рецидиве, что составляет почти половину всех состоящих под административным надзором лиц (46%).

За последние пять лет количество лиц, отбывавших наказание в виде лишения свободы за совершение преступлений террористического характера, увеличилось в 3,5 раза, экстремистской направленности — в 3,7 раз.

В настоящее время отмечается небывалое изменение структуры преступности, при котором привычные составы преступлений сократились в течение последних пяти лет на 25–35%, что создавало определенную иллюзию снижения уровня преступности. Так, в 2018 г., когда фиксировали очередное «стабильное» снижение на 3,3% уровня преступности, количество преступлений, совершаемых с использованием ИТТ, уже увеличилось в течение года

[1] См.: *Омелин В.Н.* Оперативно-розыскные мероприятия и оперативно-розыскные действия: критерии разграничения // Закон и право. 2018. № 11. С. 132–134.

почти вдвое (+92%). Аналогичная динамика наблюдается и по сей день: в 2019 г. их число возросло на 68,5%; в 2020 г. — на 73,4%. При этом более половины преступлений данной категории относятся к тяжким и особо тяжким составам, из чего следует, что значительная часть лиц, их совершивших, подпадает после освобождения из мест лишения свободы под административный надзор.

Вместе с тем установленные законом административные ограничения (нахождение в жилище в ночное время, запрет на посещение увеселительных заведений и пр.) явно не создают препятствий для продолжения поднадзорными лицами (при наличии таких намерений) противоправной деятельности с использованием сети Интернет и средств мобильной связи.

По этой причине нами было предложено законодательное закрепление названных выше оснований для проведения ОРМ, что позволило бы сотрудникам оперативных подразделений получать информацию с компьютерных устройств указанных лиц и контролировать средства связи.

Отдельным основанием для проведения ОРМ следует установить наличие неснятой или непогашенной судимости лица за тяжкое или особо тяжкое преступление до погашения или снятия судимости в установленном порядке. Одновременно в соответствующей статье, посвященной условиям проведения ОРМ, целесообразно закрепить положение, согласно которому по указанному основанию могут проводиться только ОРМ, не ограничивающие конституционные права и свободы.

В целях обеспечения соблюдения миграционного законодательства также должен осуществляться оперативно-розыскной контроль посредством сбора и проверки информации о достоверности и полноте сведений, представляемых иностранными гражданами и лицами без гражданства для легализации своего пребывания на территории государства, а также о соответствии целей прибытия и фактически осуществляемой деятельности указанных лиц требованиям национального законодательства и интересам национальной безопасности государства пребывания с момента их прибытия или письменного изъявления желания об этом в установленном порядке.

В Рекомендациях содержится конкретизация понятий конфиденциального сотрудничества с органами, осуществляющими ОРД, и конфиденциального содействия им как взаимосвязанных, но самостоятельных категорий. Это открывает возможности для межгосударственного обмена конфидентами и укрепления их социально-правовых гарантий.

Такой принципиальный подход уже закреплен в ведомственных нормативных актах МВД России, что дает положительный эффект как в части оптимизации деятельности сотрудников, соблюдения ими принципов законности и конспирации, так и с позиции финансового обеспечения. По нашему мнению, при межгосударственном обмене конфидентами целесообразно задействовать только негласных сотрудников, и только для них и специалистов, оказывающих помощь оперативно-розыскным органам на контрактной основе, следует определить порядок их допуска к сведениям, составляющим государственную тайну (по примеру Республики Беларусь). Поэтому рекомендуется закрепить в статьях, содержащих перечень понятий, используемых в законах об ОРД, следующие определения конфиденциального содействия и конфиденциального сотрудничества:

- *конфиденциальное содействие — это регулируемое законом и подзаконными актами, охраняемое государством конфиденциальное взаимодействие органа, осуществляющего оперативно-розыскную деятельность, с лицом, которое добровольно и правомерно способствует защите прав и свобод человека и гражданина, материальных и духовных ценностей общества, конституционного строя, суверенитета и территориальной целостности государства*;
- *конфиденциальное сотрудничество — это предусмотренная и охраняемая законом конфиденциальная добровольная возмездная деятельность совершеннолетнего дееспособного лица по выполнению им условий контракта, заключенного с ним органом, осуществляющим оперативно-розыскную деятельность, в целях решения ее задач.*

При разработке законодательных норм, регулирующих права и обязанности конфидентов, вопросы их социально-правовой защиты, защиты сведений о них и т.д., необходимо руководствоваться тем обстоятельством, что в данном случае речь идет о двух названных выше самостоятельных категориях.

В Рекомендациях предложено ограничить практику обязательного раскрытия перед прокурорами сведений о конфидентах при возбуждении в отношении них любого уголовного дела. Такой подход представляется нам неоправданным, в том числе в контексте обмена конфидентами в процессе межгосударственного взаимодействия в сфере ОРД.

В рамках сближения национальных законов предлагается следующая редакция рассматриваемой нормы:

«*Сведения о лицах, находящихся* (*находившихся*) *в состоянии оперативного внедрения, штатных негласных сотрудниках органов, осуществляющих оперативно-розыскную деятельность, а также о лицах, оказывающих* (*оказывавших*) *содействие этим органам либо сотрудничающих* (*сотрудничавших*) *с ними на конфиденциальной основе, представляются прокурору только с письменного согласия указанных лиц, за исключением случаев, требующих их привлечения к уголовной ответственности за совершение тяжких или особо тяжких преступлений, непосредственно связанных с оказанием содействия органу, осуществляющему оперативно-розыскную деятельность, или сотрудничеством с ним на конфиденциальной основе*».

Расхожее мнение о том, что нахождение на связи у сотрудника оперативного подразделения конфидента должно в обязательном порядке оградить последнего от совершения преступлений, не подтверждено практикой. По возможности подобные факты должны своевременно выявляться и объективно оцениваться с позиции возможности дальнейшего решения задач ОРД с привлечением данного конфидента.

В целях повышения эффективности реализации результатов ОРД по линии противодействия организованной преступности рекомендовано продление срока хранения оперативных материалов, касающихся лиц, занимающих высшее положение в преступной иерархии[1], а также лидеров террористических и экстремистских организаций.

Можно согласиться с В.Н. Фадеевым в том, что в современных условиях в ряде случаев сама организация организованной преступности поднялась на новый профессиональный уровень, который можно определить как *профессионально-организованная преступность* и охарактеризовать ее как противоправное, антиобщественное объединение социально-политической, антигосударственной направленности в экономике, социальной среде и государственном управлении, развивающее преступные технологии и контролирующее уголовную среду, выступающее как основной индикатор преступного развития общества[2].

---

[1] См.: *Гирько С.И., Белянский Е.Б.* Законодательные основы оперативно-розыскного противодействия преступлениям общеуголовной направленности, совершаемым лицами, занимающими высшее положение в преступной иерархии // Научный портал МВД России: науч. журн. М.: ВНИИ МВД России, 2016. № 3 (35). С. 52–59.

[2] *Фадеев В.Н., Тэсс Л.В.* Профессионально-организованная преступность // Вестник Москов. ун-та МВД России. 2016. № 6. С. 166–172.

Положения, содержащиеся в Рекомендациях, легли в основу предложений по совершенствованию российского оперативно-розыскного законодательства, которые в настоящее время проходят в рамках МВД России согласование в установленном порядке.

Второй этап формирования правовой основы оперативно-розыскного обеспечения коллективной безопасности связан с разработкой и нормативным закреплением конкретных направлений взаимодействия компетентных органов государств — членов ОДКБ в борьбе с преступностью.

Нами разработано модельное Соглашение государств — членов ОДКБ о сотрудничестве в сфере ОРД (далее — Соглашение), которое принято 30 октября 2018 г. на XI заседании Парламентской Ассамблеи. Соглашение содержит глоссарий из 18 терминов, среди которых помимо определения ОРД содержатся новые научно обоснованные понятия: оперативно-розыскные действия, оперативно-розыскной алгоритм, оперативно-розыскной контроль, оперативно-розыскная информация, негласный сотрудник и т.д.

Так, *оперативно-розыскные действия — это содержащиеся в национальном законодательстве государств — членов ОДКБ, помимо собственно ОРМ, организационные, управленческие и иные действия, обеспечивающие законность и эффективность ОРД.*

Значение данных действий в условиях освоения новых ИТТ постоянно повышается, особенно в сфере оперативно-розыскной аналитики, что является общеевропейской тенденцией[1]. Так, в июне 2017 г. в Вене было принято Руководство ОБСЕ по полицейской деятельности на основе оперативных данных и информации[2], в котором отмечен ряд моментов, обосновывающих необходимость существенной оптимизации процесса борьбы с преступностью.

Во-первых, очевидны серьезные сложности, с которыми сталкиваются традиционные модели правоохранительной деятельности, основанные на реагировании на уже произошедшие инциденты. Современные опасности и угрозы обусловлены повышением мобильности и миграции населения, быстрыми технологическими и коммуникационными изменениями, свободным перемещением товаров и услуг, растущим неравенством в доходах. Они диктуют необходимость изменения парадигмы правоохранительной дея-

---

[1] См.: *Овчинский В.С.* Виртуальный щит и меч: США, Великобритания, Китай в цифровых войнах будущего. М., 2018.

[2] Руководства ОБСЕ по полицейской деятельности на основе оперативных данных и информации // Серия публикаций Секретариата ОБСЕ. Департамент по противодействию транснациональным угрозам. Отдел стратегических вопросов полицейской деятельности. 13-е изд.

тельности посредством ее переориентирования на меры упреждающего, превентивного характера.

Во-вторых, насильственный экстремизм и радикализация, ведущие к терроризму, террористические атаки последних лет подчеркивают необходимость обмена, интеграции и централизованного анализа соответствующих данных и информации (оперативных материалов) всех уровней в соответствии с национальными законодательствами, международными стандартами в области прав человека и обязательствами ОБСЕ.

Осуществление на системной основе предиктивной функции полиции должно включать в себя оперативно-розыскной контроль[1], связанный с оперативно-профилактическим наблюдением за поведением лиц, ранее судимых, в первую очередь тех, которые представляют угрозу коллективной безопасности государств — членов ОДКБ. Именно на такой методологической основе разработано понятие данной категории.

Так, *оперативно-розыскной контроль — это система комплексов оперативно-розыскных мероприятий и действий, осуществляемых в соответствии с национальным законодательством Сторон и настоящим Соглашением в отношении ранее судимых лиц из числа организаторов и активных участников преступной деятельности, связанной с терроризмом, экстремизмом, незаконным оборотом наркотических средств и психотропных веществ, огнестрельного оружия, взрывчатых веществ и взрывных устройств, фальшивомонетничеством, незаконной миграцией, киберпреступностью, а также участников миграционных потоков, заключающихся в оперативно-профилактическом наблюдении за их образом жизни и поведением в целях предупреждения и пресечения совершения ими преступлений, выявления в их среде преступников и лиц, представляющих оперативный интерес для Сторон, недопущения вовлечения их в преступную деятельность другими лицами и причинения ими ущерба национальной и коллективной безопасности государств — членов ОДКБ.*

Развитие организации и тактики ОРД в условиях информационного общества, с учетом осложнения условий, в которых осуществляют свою деятельность сотрудники оперативных подразделений, что связано с постоянным дефицитом времени для принятия решений, а также многообразием и сложностью стоящих перед ними задач, невозможно без ее алгоритмизации.

---

[1] См.: *Маслов А.А., Бабушкин А.А.* Система оперативно-розыскного контроля органов внутренних дел за лицами, склонными к совершению тяжких и особо тяжких преступлений: монография. М.: ВНИИ МВД России, 2016.

По этой причине в Соглашение включено понятие «*оперативно-розыскной алгоритм*», *под которым понимается научно обоснованный и апробированный на практике нормативно закрепленный организационно-тактический комплекс необходимых* (*обязательных*) *оперативно-розыскных мероприятий и действий, осуществляемых в целях решения задач ОРД государств — членов ОДКБ и развития системы их коллективной безопасности.*

В Соглашении закреплены принципы оперативно-розыскного обеспечения коллективной безопасности или межгосударственного сотрудничества в сфере ОРД, к которым относятся: суверенное равенство Сторон и невмешательство в их внутренние дела; законность; уважение и соблюдение прав и свобод человека и гражданина; конспирация; сочетание гласных и негласных методов и средств; наступательность в вопросах обеспечения национальной и коллективной безопасности.

Определены 22 направления взаимодействия компетентных органов Сторон и порядок их реализации, связанные с информационным обменом, выполнением запросов, проведением скоординированных ОРМ, в том числе при получении специальных уведомлений из Генерального секретариата Интерпола, пресечением каналов сбыта оружия, наркотиков, финансирования экстремизма и терроризма, обеспечением оперативно-розыскного контроля за ранее судимыми лицами, представляющими опасность для объектов коллективной безопасности, разработкой и применением оперативно-розыскных алгоритмов, принятых в качестве стандартов в целях повышения защищенности критически важных объектов, влияющих на национальную безопасность нескольких или всех государств — членов ОДКБ.

Пандемия COVID-19 показала значимость обеспечения биологической безопасности, в рамках которой должны решаться вопросы предупреждения диверсий на потенциально опасных биологических объектах, а также совершения террористических актов и диверсий с использованием патогенов[1].

Кроме того, предусматривается обмен негласными сотрудниками, результатами ОРД, опытом в сфере организации и тактики выявления, предупреждения, пресечения и раскрытия преступлений.

Межгосударственное сотрудничество в сфере ОРД также предполагает совместное финансирование и проведение научно-ис-

[1] Статья 12 Федерального закона от 30 декабря 2020 г. № 492-ФЗ «О биологической безопасности в Российской Федерации».

следовательских и опытно-конструкторских работ по разработке эффективных методик и специальных технических средств, программных комплексов и средств защиты оперативно-розыскной информации, а также организацию профессиональной подготовки и повышения квалификации сотрудников оперативных подразделений Сторон. Данный перечень является открытым и практика межгосударственного сотрудничества, в том числе в условиях освоения новых ИТТ, разовьет и обогатит содержание оперативно-розыскного обеспечения коллективной безопасности.

Таким образом, в заключение можно отметить, что в результате проведенного исследования разработаны основные понятия в исследуемой сфере, в том числе понятие оперативно-розыскного обеспечения коллективной безопасности, его цели и задачи, принципы, система и содержание.

Так, *оперативно-розыскное обеспечение коллективной безопасности государств — членов ОДКБ — это осуществление в соответствии с национальным законодательством и настоящим Соглашением компетентными органами государств — членов ОДКБ оперативно-розыскных мероприятий и действий, направленных на защиту жизни, здоровья, прав и свобод человека и гражданина, обеспечение общественной и государственной безопасности в зоне ответственности ОДКБ путем использования оперативно-розыскных сил, средств и методов.*

Задачами оперативно-розыскного обеспечения коллективной безопасности государств — членов ОДКБ являются:

— выявление, предупреждение, пресечение и раскрытие преступлений, подготавливаемых, совершаемых или совершенных в зоне ответственности ОДКБ, связанных с терроризмом, экстремизмом, наемничеством, организованной преступностью, коррупцией, незаконным оборотом наркотиков и оружия, киберпреступностью, незаконной миграцией и иными общественно опасными деяниями;

— розыск лиц, скрывающихся от органов дознания, следствия и суда государств — членов ОДКБ, уклоняющихся от наказания, а также розыск без вести пропавших в данных государствах лиц;

— сбор сведений о событиях и действиях (бездействии), создающих угрозу коллективной и национальной безопасности государств — членов ОДКБ;

— пресечение в зоне ответственности ОДКБ каналов финансирования терроризма и экстремизма, поступления наркотиков и оружия, установление местонахождения имущества, подлежа-

щего конфискации в связи с совершением данных преступлений, а также коррупции;

— выявление лиц — носителей угроз для коллективной и национальной безопасности, осуществление за ними непрерывного оперативно-розыскного контроля;

— защита от преступных посягательств критически важных и иных особо важных объектов, а также потенциально опасных биологических объектов, на которых осуществляется деятельность с использованием патогенов.

Сближение и гармонизация законов об ОРД государств — членов ОДКБ, принятие ими указанного Соглашения создают условия для формирования системы оперативно-розыскного обеспечения коллективной безопасности и определения основных направлений сотрудничества.

Система оперативно-розыскного обеспечения коллективной безопасности государств — членов ОДКБ — это совокупность задействованных в установленном национальными законами об ОРД и настоящим Соглашением порядке в целях обеспечения коллективной безопасности государств — членов ОДКБ сил и средств их компетентных органов (*в том числе создаваемые по их решению объединенные оперативно-розыскные группы и привлекаемые негласные сотрудники*), *проводимых ими ОРМ и действий, а также используемых форм и методов.*

В соответствии с данным определением *силы оперативно-розыскного обеспечения коллективной безопасности* составляют:

- оперативные подразделения органов, осуществляющих ОРД, государств — членов ОДКБ (компетентные органы);
- объединенные оперативно-розыскные группы, создаваемые по решению компетентных органов;
- негласные сотрудники (лица, конфиденциально содействующие компетентным органам и сотрудничающие с ними).

Организационно-тактические формы оперативно-розыскного обеспечения коллективной безопасности — это комплексы оперативно-розыскных мероприятий и действий, проводимых компетентными органами государств — членов ОДКБ по соответствующим направлениям межгосударственного сотрудничества в сфере ОРД, нацеленные на обеспечение коллективной безопасности данных государств.

Ход исследования и процесс разработки рассмотренных выше документов рекомендательного характера неоднократно обсуждались на заседаниях Экспертно-консультативного совета и Постоянной комиссии по социально-экономическим и правовым во-

просам Парламентской Ассамблеи ОДКБ, а также докладывались во ВНИИ МВД России, Академии МВД Республики Беларусь и Краснодарском университете МВД России.

Одним из наиболее дискуссионных остается вопрос проведения оперативными подразделениями государств — членов ОДКБ совместных ОРМ и возможности участия в их проведении представителей компетентных органов одного государства на территории другого.

Данный вопрос, несмотря на активную позицию представителей МВД Республики Таджикистан, направленную на более тесную интеграцию деятельности оперативно-розыскных органов, пока не получил общей поддержки представителей государств — членов ОДКБ, в результате чего временно выведен за рамки Соглашения.

Напомним, что в соответствии со ст. 8 Конвенции о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам (Кишинев, 7 октября 2002 г.) представители компетентного органа запрашивающей Стороны могли не только присутствовать при осуществлении процессуальных и розыскных действий, которые проводят компетентные органы запрашиваемой Стороны, но также, если это не противоречит национальному законодательству принимающего государства, принимать в них участие.

Однако в современных условиях такую позицию не поддерживают некоторые государства, ссылаясь на то, что правовой статус представителя иного государства в качестве участника ОРМ в их законодательстве не определен (Республика Беларусь).

В ст. 17 Конвенции Шанхайской организации сотрудничества по противодействию экстремизму (Астана, 9 июня 2017 г.) определено, что Сторона, осуществляющая преследование лиц, подозреваемых или обвиняемых в совершении преступлений, охватываемых Конвенцией, и установившая, что эти лица находятся на территории другой Стороны, может при получении разрешения компетентных органов этой Стороны направить своих сотрудников на территорию запрашиваемой Стороны для присутствия при осуществлении ОРМ и следственных действий.

Аналогичная позиция закреплена в проекте Соглашения и одобрена правоохранительными органами государств — членов ОДКБ.

В настоящее время с учетом анализа плановых документов Парламентской Ассамблеи Организации государств — членов ОДКБ можно сделать вывод о том, что термин оперативно-розыскного обеспечения коллективной безопасности прочно вошел в практику международного сотрудничества.

Так, в Программе деятельности Парламентской Ассамблеи Организации Договора о коллективной безопасности по сближению и гармонизации национального законодательства государств — членов ОДКБ на 2021–2025 г. запланированы:

- во-первых, разработка Модельного Руководства компетентных органов государств — членов ОДКБ в сфере оперативно-розыскного обеспечения коллективной безопасности;
- во-вторых, проведение межгосударственного круглого стола (конференции) по теме: «Оперативно-розыскное обеспечение коллективной безопасности государств — членов ОДКБ в условиях информационного общества и пути его совершенствования», с выпуском сборника по данной теме.

Осуществление данных мероприятий должно послужить дальнейшему совершенствованию теоретико-правовой основы оперативно-розыскного обеспечения коллективной безопасности государств — членов ОДКБ, а также наполнению его практической организационно-тактической, информационно-аналитической составляющей.

Раздел IV
ИСПОЛЬЗОВАНИЕ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ОПЕРАТИВНО-РОЗЫСКНОЙ ДЕЯТЕЛЬНОСТИ НА ОСНОВНЫХ НАПРАВЛЕНИЯХ БОРЬБЫ С ПРЕСТУПНОСТЬЮ

А.В. Морозов

Актуальные вопросы оперативно-розыскной деятельности по борьбе с незаконным наркопроизводством в современной России в условиях цифровой реальности

Одной из угроз национальной безопасности России в сфере оборота наркотиков и в области противодействия их незаконному обороту признаны увеличение предложения на рынке сбыта (в целях незаконного потребления) синтетических наркотиков, произведенных на территории Российской Федерации с применением веществ, часто используемых при производстве, изготовлении и переработке наркотических средств и психотропных веществ и находящихся в законном обороте, а также рост спроса на такие наркотики[1].

Этот вывод подтверждается официальной статистикой. Так, за последние 11 лет, при снижении почти в 2 раза общего количества изъятых правоохранительными органами наркотиков в России (с 41 т 245,8 кг в 2010 г. до 20 т 965,9 кг в 2020 г.), количество изъятых синтетических наркотиков возросло в 17 раз (с 506,3 кг в 2010 г. до 8 т 663,5 кг в 2020 г.)[2]. Доля синтетических наркотиков от общего количества изъятых наркотиков соответственно выросла с 1,2 до 41,3%.

В результате проведения ОРМ и следственных мероприятий в течение 2020 г.[3] правоохранительными органами России из незаконного оборота изъято 20 т 966 кг наркотических средств, из которых 8 т 663 кг (или 41,3%) приходится на синтетические наркотические средства, а также 559,9 кг психотропных веществ. За ана-

[1] Пункт «д» ст. 9 Стратегии антинаркотической политики Российской Федерации на период до 2030 года, утвержденной Указом Президента РФ от 23 ноября 2020 г. № 733.

[2] Здесь и далее сведения о количестве изъятых подконтрольных веществ на территории Российской Федерации приводятся в соответствии с данными межведомственной статистической отчетности ГИАЦ МВД России за 2010–2020 годы (форма № 3-МВ-НОН (173), книга 1).

[3] Здесь и далее сведения о количестве изъятых подконтрольных веществ на территории РФ приводятся в соответствии с данными ГИАЦ МВД России с января по декабрь 2019 г. и с января по декабрь 2020 г. (форма № 3-МВ-НОН (173)).

логичный период предыдущего года в России изъято 19 т 470 кг наркотических средств, из них лишь 5 т 142 кг — синтетического происхождения (26,4% от общего количества изъятого), а также 372,4 кг психотропных веществ. Еще заметнее увеличилась доля синтетических наркотиков, изъятых в прошедшем году ОВД: с 2 т 597 кг в 2019 г. (17,8% от всего количества изъятых наркотических средств (14 т 614 кг)) до 7 т 804 кг в 2020 г. (43,1% от всего количества (18 т 118 кг)).

28 февраля 2019 г., выступая на расширенном заседании коллегии МВД России «О результатах деятельности МВД России за 2018 год», Президент России В.В. Путин отметил: «Одной из ключевых задач МВД остается противодействие незаконному обороту наркотиков. Статистика показывает, что масштаб распространения наиболее опасных — синтетических наркотиков растет. Это тревожный сигнал. Мы должны иметь в виду, учитывать его. Нужно принимать дополнительные меры, потому что тех, что есть, видимо, недостаточно для эффективной работы. Необходимо активно пресекать работу наркодилеров, выявлять организованные преступные группы, связанные с ввозом наркотиков из-за границы, их производством внутри нашей страны. В этой работе прошу тесно взаимодействовать с Федеральной службой безопасности, Федеральной таможенной службой и другими ведомствами, а также с коллегами из-за рубежа».

Наиболее популярными у наркопроизводителей в последние годы являются мефедрон, производное N-метилэфедрона, α-PVP и амфетамин.

Так, в 2020 г. наркотики катиноновой группы заняли лидирующие позиции (количество выявленных нарколабораторий по производству мефедрона и N-метилэфедрона составляет свыше 83%, амфетамина — только 11%).

Количество N-метилэфедрона в течение 2020 г. по сравнению с анализируемым периодом прошлого года увеличилось примерно в 2,5 раза (на 164,2%) и составило 5 т 640 кг (2019 г. — 2 т 135 кг). ОВД изъято 5 т 414 кг N-метилэфедрона, что на 262,6% больше, чем в 2019 г. (1 т 493 кг).

На втором месте по распространенности среди синтетических наркотиков — мефедрон. С января по декабрь 2020 г. количество наркотика данного вида, изъятого правоохранительными органами, увеличилось на 194,8% и составило 2 т 315 кг (2019 г. — 785,4 кг); ОВД изъято 1 т 806 кг мефедрона, что на 309,6% превысило показатель 2019 г. — 440,9 кг.

Следующую после N-метилэфедрона и мефедрона позицию занимают синтетические аналоги тетрагидроканнабинола (далее — ТГК). Однако следует отметить снижение популярности среди потребителей, кроме того, данные вещества не изготавливаются внутри страны, а поставляются из-за границы, что в условиях закрытия границ ввиду пандемии существенно укрепило тенденцию снижения их количества в незаконном обороте. Так, за анализируемый период правоохранительными органами изъято 120,5 кг синтетических аналогов ТГК (2019 г. — 248,2 кг, снижение на 51,5%), ОВД — 90,9 кг (2019 г. — 126,8 кг, снижение на 28,3%).

Если ранее наибольшее количество синтетических наркотиков изымалось в крупных промышленных центрах, то в настоящее время наиболее значительные изъятия территориально сместились в районы, расположенные в непосредственной близости от наиболее крупных городов страны — Москвы и Санкт-Петербурга, поскольку на их территории наиболее удобно размещать нарколаборатории, а произведенную продукцию прятать в крупные тайники (закладки) в лесном массиве.

Возможность оборудования обособленного помещения в таких местах удачно сочетается с относительно развитой транспортной инфраструктурой и близостью крупнейших мегаполисов, где можно закупать необходимое оборудование и реактивы, одновременно сбывая изготавливаемый «продукт».

Так, в течение 2020 г. в Москве изъято 172,6 кг синтетических наркотических средств (ОВД — 169,9 кг), в Санкт-Петербурге — 93,6 кг (ОВД — 87,5 кг), в то время как в Ленинградской области изъято 3 т 229 кг (ОВД — 3 т 172 кг), в Московской области — 834,7 кг (ОВД — 588,6 кг), во Владимирской области — 634,1 кг (ОВД — 622,2 кг), в Ивановской области — 245,7 кг (ОВД — 204,2 кг), в Тульской области — 106,3 кг (ОВД — 105,5 кг).

В итоге «классические», ранее хорошо известные наркотики (гашиш, марихуана, героин, кокаин) постепенно замещаются их синтетическими более дешевыми аналогами, изготовленными внутри страны и являющимися не менее опасными для здоровья граждан.

Причиной такой ситуации в том числе является то, что изготовление синтетических психоактивных веществ в подпольных лабораториях оказывается для наркодилеров рентабельнее и безопаснее, чем их контрабанда. Нет расходов на изготовление специальных тайников, транспортных расходов, оплаты труда курьеров, риска изъятия партии наркотиков и транспортного средства таможенниками или пограничниками при пересечении границы

и в ходе досмотра на автотрассах сотрудниками ДПС ГИБДД ОВД, задержания при этом курьеров. Отсутствует потребность в дорогостоящем оборудовании и необходимость наличия особых климатических условий для культивирования наркосодержащих растений (как, например, в случаях с коноплей, опийным маком, кокаиновым кустом или с псилоцибин-содержащими грибами). При этом подпольное наркопроизводство может быть глубоко законспирировано и без особых затрат (используются обычные неприметные гаражи, частные дома, боксы и склады хранения, заброшенные цеха, а также другие труднодоступные и скрытые от правоохранительных органов места).

Например, *в ноябре 2019 г. при проведении рейда в рамках оперативно-профилактического мероприятия «Мигрант» участковым уполномоченным полиции в одном из поселков Тосненского р-на Ленинградской обл. в складском помещении обнаружена крупнейшая нарколаборатория по производству синтетических наркотиков. Изъято 3 т 046,250 кг α-PVP, значительное количество прекурсоров и иных химических реактивов, а также пять реакторов для процесса химического синтеза, автопогрузчик, три грузовых автотранспортных средства.*

Осенью 2018 г. участники преступной группы с целью сокрытия преступных замыслов по созданию нарколаборатории выкупили участок территории бывшего Касимовского судоремонтного завода в Рязанской области площадью 1 га, представляющий собой полуостров на р. Ока, на который ведет только одна труднопроходимая дорога. Находящееся на участке заброшенное помещение оборудовали электрогенератором, вытяжкой, приспособлениями для слива и забора речной воды с фильтрами, установили в нем современное профессиональное химическое оборудование, стоимость которого превышает 1,5 млн руб. Преступники, проявляя осведомленность о методах оперативно-розыскной деятельности, при изготовлении наркотиков действовали с повышенной осторожностью, проводя проверочные мероприятия через сеть информаторов, включая отдельных сотрудников охраны бывшего завода. В целях скрытой перевозки «сырья» для изготовления наркотиков, а также готовой продукции приобрели два автомобиля, оборудовав их тайниками. По предварительной оценке, производительность лаборатории составляла от 10 до 20 кг (примерно от 30 до 60 тыс. разовых доз) высококонцентрированных синтетических наркотиков (амфетамина и мефедрона) в неделю и приносила ее организаторам еженедельный доход не менее 10 млн руб. Произведенные наркотики сбывались крупным оптом через сеть «Даркнет» тайниково-закладочным

способом на территории различных регионов России. В ходе спецоперации, проведенной 26–27 февраля 2019 г., участники группы задержаны «с поличным». В лаборатории обнаружено и изъято свыше 30 кг готовой «синтетики», более 100 кг наркосодержащих жидкостей, 500 кг прекурсоров, 60 единиц специального химического оборудования, банковские карты, ноутбуки, смартфоны, а также автотранспортные средства, которые использовались в преступной деятельности[1].

Для участия в наркопроизводстве не требуется обширных специальных познаний. Приобретение оборудования и большей части необходимых компонентов, с развитием ИКТ и широкого круга услуг по почтовой и курьерской доставке, не вызывает существенных затруднений.

Так, в последнее время набирают популярность так называемые «конструкторские» лаборатории, которые могут создаваться для однократного получения психоактивных веществ из так называемых «конструкторов» — специальных наборов реагентов для получения определенного количества и вида синтетических наркотиков в одну-две стадии. Синтез осуществляется непосредственно в самих емкостях, входящих в набор, либо с применением любых подручных средств — чашек, банок, мисок, кружек, стаканов. Лаборатории данного вида не имеют постоянного местонахождения и в зависимости от предпочтений участников преступного синтеза могут создаваться на время в любом месте. Участники синтеза обычно не имеют специальных знаний в химии и действуют по подробной инструкции на упаковке «конструктора». Из одного набора однократно изготавливается психоактивное вещество в четко определенном количестве, так как необходимые для него реагенты и прекурсоры строго ограничены и рассчитаны.

Так, 19 сентября 2018 г. в Кемерово в ходе обследования квартиры одного из местных жителей изъято 1 кг 722,2 г производного N-метилэфедрона, изготовленного им в подпольной нарколаборатории, находящейся в дачном домике СНТ «Огонек» п. Черемичкино Топкинского района.

В докладе 62-й сессии Комиссии ООН по наркотическим средствам (7 декабря 2018 г., 14–22 марта 2019 г.) отмечается, что, наряду с расширением и диверсификацией ассортимента и рынка наркотиков, производство и изготовление, незаконный оборот

[1] Особенности борьбы с незаконным изготовлением и производством синтетических наркотиков в условиях подпольных лабораторий: учеб.-практич. пособие / А.В. Морозов [и др.]; сост. В.Г. Дикарев. Домодедово: ВИПК МВД России, 2019.

наркотиков и их прекурсоров достигли рекордного уровня, а незаконный спрос на химические вещества — прекурсоры и масштабы их утечки из каналов внутреннего распределения растут.

Вызывает обеспокоенность еще одна современная тенденция.

Еще несколько лет назад подавляющее большинство наркотических средств и психотропных веществ, в том числе синтетического происхождения, поступало на территорию государства контрабандным путем извне (например, синтетические каннабиноиды из КНР, МДМА из Нидерландов). Факты незаконного производства наркотиков с целью их последующего распространения неопределенному кругу лиц являлись скорее исключением, чем правилом. Однако в настоящее время ситуация кардинально изменилась.

Рост количества подпольных нарколабораторий в 2020 г. спровоцирован в основном закрытием границ в связи с противодействием пандемии COVID-19, что отразилось на ранее существовавших логистических схемах контрабандного ввоза на территорию России готовых наркотиков синтетического, полусинтетического и растительного происхождения. Следует отметить, что меры, принятые российскими властями для борьбы с коронавирусом, практически не сказались на состоянии наркорынка наркотиков катиноновой группы, таких как мефедрон и другие популярные синтетические наркотики, поскольку они синтезируются внутри страны, а их необходимые химические элементы производятся легально на отечественных химических предприятиях в городах Омске и Челябинске.

Таким образом, в условиях пандемии на место основного источника поступления синтетических наркотиков в незаконный оборот в России выдвинулось внутреннее наркопроизводство при одновременном снижении роли контрабанды.

Организация нелегальных лабораторий по производству синтетических наркотиков, совершенствование синтеза и рост объемов внутреннего наркопроизводства существенно увеличивают их предложение в незаконном обороте России.

В результате анализа причин и условий такой ситуации в 2020 г. были выделены ряд проблемных вопросов, способствующих росту внутреннего наркопроизводства.

1. *Использование в наркопроизводстве химических реактивов, не включенных в Перечень подконтрольных веществ*[1]

[1] Перечень утвержден постановлением Правительства РФ от 30 июня 1998 г. № 681 «Об утверждении перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации», далее — Перечень.

в качестве прекурсоров. Совершенствование мер контроля над прекурсорами на глобальном уровне вынудило организаторов подпольных нарколабораторий разработать ряд контрстратегий, включая применение более сложных способов приобретения химических веществ — прекурсоров и замену их неконтролируемыми «предпрекурсорами» для изготовления необходимых им прекурсоров. В таких случаях изготовление наркотиков, как правило, усложняется лишь на один цикл, в ходе которого из легальных веществ[1] сначала изготавливаются необходимые для производства конечного наркотика прекурсоры. Преимущественно данные вещества используются в промышленности, свободно реализуются через крупные химбазы и магазины торговли химической продукцией (в том числе оптовые). Многие из таких магазинов специализируются на реализации химических «конструкторов» и активно продвигают свои услуги через сеть Интернет. В целях конспирации юридические лица, торгующие химическим оборудованием и реактивами, в том числе через интернет-магазины, часто меняют наименования и фактические адреса расположения, что затрудняет процесс принятия соответствующих мер контроля и проведения оперативно-розыскных мероприятий.

2. *Законодательно закрепленная концентрация многих прекурсоров, при которой за их незаконный оборот предусмотрена уголовная ответственность.* Анализ практики незаконного наркопроизводства показывает, что многие прекурсоры списка I и таблицы I списка IV Перечня легально реализовывались, а некоторые и в настоящее время реализуются в законодательно не запрещенной концентрации (т.е. в концентрации (10–40%), при которой не наступает уголовная ответственность за незаконный оборот). В 2018–2019 гг. по инициативе ГУНК МВД России Правительством Российской Федерации отменены требования к концентрации в отношении ряда прекурсоров Перечня[2]. Данная мера до-

[1] Например, «4-метилвалерофенон», «4-фторвалерофенон», «3,4-диметилвалерофенон», «3,4-метилендиоксивалерофенон», «4-метоксивалерофенон» и др. (приведены торговые названия). Такие вещества еще называют «предпрекурсоры».

[2] Постановления Правительства РФ от 28 марта 2018 г. № 337 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с совершенствованием контроля за оборотом прекурсоров наркотических средств и психотропных веществ», от 22 февраля 2019 г. № 182 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с совершенствованием контроля за оборотом прекурсоров наркотических средств и психотропных веществ».

казала свою эффективность. Так, с сентября 2018 г. у сотрудников правоохранительных органов появились законные основания для изъятия одного из основных веществ, используемых в синтезе амфетамина — 1-фенил-2-нитропропена (в любой концентрации), что привело к значительному сокращению числа «амфетаминовых» лабораторий, поскольку поиск заменителей (аналогов) для синтеза данного психотропного вещества требует специальных знаний в области химии и определенных дополнительных финансовых затрат. Как следствие, с конца 2018 г. наблюдается резкое снижение в незаконном обороте этого психотропного вещества. Так, в 2018 г. правоохранительными органами его изъято 586,3 кг, в 2019 г. — 361,1 кг, в 2020 г. — 340,5 кг.

3. *Отсутствие в экспертных подразделениях стандартных (эталонных) контрольных образцов значительной части подконтрольных прекурсоров.* В Перечне сохраняются позиции контролируемых прекурсоров с оговоркой об их концентрации[1]. Особенно это актуально для часто используемых в подпольных лабораториях бензальдегида и нитороэтана. Такое несовершенство нормативного правового регулирования оборота прекурсоров создает проблемы в определении экспертными подразделениями МВД России процентной концентрации прекурсоров ввиду отсутствия соответствующих стандартных образцов.

4. *Отсутствие в ФТС России информации о поставках прекурсоров и других химических реактивов, используемых в наркопроизводстве.* Отслеживание их поступления в Россию из-за рубежа, например из КНР, весьма затруднительно, поскольку в таможенных документах такие вещества декларируются обобщенными наименованиями, например «ароматические кетоны», без указания конкретной химической формулы. Кроме того, пресечение таких поставок затруднено в силу больших объемов товаров, перемещаемых через границу.

5. *Совершенствование и доступность к покупке в розницу современного специального химического оборудования.* Масштабное наркопроизводство невозможно без использования специальных инструментов и лабораторного оборудования. В соответствии со ст. 8 Федерального закона от 8 января 1998 г. № 3-ФЗ «О наркотических средствах и психотропных веществах» соответствующие вопросы регулирует постановление Правительства РФ

[1] В таблице I списка IV Перечня — 19 прекурсоров с требованиями к концентрации.

от 22 марта 2001 г. № 221[1], в том числе перечень такого оборудования и инструментов и правила их оборота[2], согласно которым: разработка, производство, изготовление, перевозка, пересылка инструментов и оборудования осуществляются в соответствии с отраслевыми нормативами, установленными для этих категорий работ; распределение инструментов и оборудования по организациям осуществляется Минпромторгом России в установленном порядке, а их ввоз в Российскую Федерацию, вывоз из Российской Федерации, отпуск, реализация и приобретение производятся организациями по согласованию с указанным Министерством. За нарушение правил оборота инструментов и специального оборудования предусмотрена административная[3] и уголовная ответственность[4]. В Перечень инструментов и оборудования, находящихся под специальным контролем и используемых для производства и изготовления наркотических средств, психотропных веществ, включены лишь оборудование для прессования таблеток и наполнения ампул (четыре наименования). Вместе с тем в большинстве случаев подтверждены факты использования в подпольных лабораториях химических реакторов, магнитных мешалок, вакуумных насосов, обратных холодильников в качестве основного и необходимого оборудования для незаконного производства наркотических средств, психотропных веществ и их прекурсоров. С учетом востребованности лабораторного оборудования в промышленности установление мер контроля за его продажей физическим и юридическим лицам может быть

[1] «Об утверждении перечня инструментов и оборудования, находящихся под специальным контролем и используемых для производства и изготовления наркотических средств, психотропных веществ, и Правил разработки, производства, изготовления, хранения, перевозки, пересылки, отпуска, реализации, распределения, приобретения, использования, ввоза в Российскую Федерацию, вывоза из Российской Федерации, уничтожения инструментов и оборудования, находящихся под специальным контролем и используемых для производства и изготовления наркотических средств, психотропных веществ».

[2] Правила разработки, производства, изготовления, хранения, перевозки, пересылки, отпуска, реализации, распределения, приобретения, использования, ввоза в Российскую Федерацию, вывоза из Российской Федерации, уничтожения инструментов и оборудования, находящихся под специальным контролем и используемых для производства и изготовления наркотических средств, психотропных веществ, утвержденные постановлением Правительства РФ от 22 марта 2001 г. № 221.

[3] Статья 6.15 Кодекса Российской Федерации об административных правонарушениях (далее — КоАП РФ).

[4] Статья 228.2 Уголовного кодекса Российской Федерации.

реализовано путем лицензирования деятельности по розничной торговле отдельными видами специального лабораторного оборудования с обязательной идентификацией и регистрацией персональных данных его покупателей (физических и юридических лиц), а также путем подготовки соответствующего постановления Правительства РФ, определяющего список специального лабораторного оборудования, общие меры по его контролю, и внесения соответствующих дополнений в статьи ряда федеральных законов[1].

6. *Все чаще для обеспечения бесперебойной работы нарколабораторий участники преступных групп осуществляют доставку химических реактивов, прекурсоров и лабораторного оборудования с использованием услуг различных мелких курьерских служб, что существенно осложняет установление конечных получателей и каналов поступления.* Кроме того, для конспирации изменяются установочные данные как грузоотправителей, так и грузополучателей. Нередко используются подложные документы, выполненные из бланков паспортов, находящихся в розыске, а также документы так называемых «фирм-однодневок».

7. *Использование участниками преступных групп для реализации подконтрольных прекурсоров, лабораторного оборудования и готовых наркотиков современных ИКТ.* Запрещенные к обороту прекурсоры, а также «конструкторы» в значительной части случаев заказываются в специально организованных интернет-магазинах через международную интернет-площадку «Гидра» и распространяются тайниково-закладочным способом или через услуги транспортных компаний или сеть специальных курьеров. Кроме того, в сети Интернет распространяется информация

[1] Статьи 1 и 8 Федерального закона от 08.01.1998 № 3-ФЗ (о закреплении понятия «специальное лабораторное оборудование», а также необходимости лицензирования деятельности, связанной с оборотом отдельных видов лабораторного оборудования); ст. 12 Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» (относительно деятельности по продаже специального лабораторного оборудования); ст. 18 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» (установление обязанности оператора по проверке подлинности предоставления персональных данных); п. 38 ст. 13 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» (наделение сотрудников полиции правом проведения проверок юридических лиц, осуществляющих покупку и продажу лабораторного оборудования, используемого в незаконном производстве наркотических средств, психотропных веществ и их прекурсоров); ст. 13.11 КоАП РФ (установление ответственности юридических и физических лиц за предоставление недостоверных персональных данных оператору).

о методах изготовления и наркопроизводства (схемах синтеза), необходимой конспирации для этого. При помощи мессенджеров («Imo», «CoverME», «Signal», «Vipole», «TikTok») осуществляется общее руководство наркопроизводством, в том числе поступают заказы на изготовление, даются указания об отправке готовой партии курьером или оборудовании соответствующих оптовых тайников-закладок с изготовленными наркотиками[1]. В сети Интернет осуществляется активная вербовка изготовителей и курьеров. Оплата их услуг и легализация наркодоходов осуществляются через электронные платежные системы и биржи криптовалют.

Например, ГУНК МВД России совместно с УНК ГУ МВД России по Волгоградской области в 2020 г. пресечена деятельность межрегионального преступного сообщества, специализирующегося на незаконном производстве и последующем распространении наркотиков на территориях Московской, Владимирской, Волгоградской, Курской, Воронежской, Оренбургской, Челябинской, Астраханской областей и Республики Татарстан тайниково-закладочным способом через интернет-магазин «X–LAB», при этом во Владимирской области ликвидирована нарколаборатория, из которой поставлялись синтетические наркотики для последующего сбыта, изъято 35 кг наркотиков.

5 марта 2021 г. в Тобольском районе Тюменской области задержан О., который работал в интересах теневого интернет-магазина «Yello Syndicate» в качестве изготовителя синтетических наркотиков в условиях подпольной лаборатории. Получение необходимых химических реагентов и лабораторного оборудования, а также поставки уже изготовленных партий наркотиков осуществлялись через «тайники-закладки» с использованием мессенджера «Jabber».

8. *Недостаточный уровень профессиональных знаний сотрудников полиции в области борьбы с незаконным производством наркотиков и соблюдения мер личной безопасности при работе с используемыми наркопроизводителями химикатами, опасными для жизни и здоровья*. Борьба с наркопроизводством, в том числе выявление подпольных нарколабораторий и сбор доказательств в отношении изготовителей наркотиков — это сложный, многоплановый, комплексный и инициативный процесс. МВД России на постоянной основе проводит анализ и прогнозирует раз-

[1] Оптовые «закладки» обычно хорошо спрятаны, чаще всего зарыты в землю, делаются в труднодоступных местах, вдали от населенных пунктов (лес, открытое поле), что затрудняет проведение ОРМ.

витие наркоситуации в сфере оборота синтетических наркотиков и их прекурсоров, организовано взаимодействие с ФСБ России и ФТС России. В области регулирования легального оборота веществ проводится работа с Минпромторгом и Минздравом России.

В последнее время существенно активизирована оперативно-служебная деятельность подразделений наркоконтроля в сфере выявления и ликвидации подпольных нарколабораторий и борьбы с наркопроизводством, что позволило достигнуть определенных результатов.

Так, за семь лет выявление таких мест ОВД увеличилось в 5,5 раз (с 33 до 182). Всего таких мест ликвидировано 754.

На существенную активизацию работы правоохранительных органов в сфере борьбы с наркопроизводством в последние годы указывает официальная статистика. Так, за последние 11 лет (с 2010 г.) наблюдается увеличение в 7,2 раза количества фактов возбуждения уголовных дел по ст. 228.1 УК РФ в части незаконного производства наркотиков, особенно после 2017 г. А по итогам 2020 г. этот показатель достиг рекордного значения — 500[1].

Например, в результате проведенных в ноябре 2019 г. мероприятий установлено, что на территории Московской, Новосибирской, Тверской, Владимирской, Курской, Калужской, Архангельской областей, республик Татарстан и Бурятия, Хабаровского и Приморского краев, а также ряда других регионов действует преступная группа, участниками которой налажены производство синтетических наркотиков в условиях подпольной лаборатории и их дальнейший сбыт. За непродолжительное время пресечено 18 поставок наркотиков в регионы РФ, привлечено к уголовной ответственности 35 лиц, в четырех регионах ликвидированы розничные сети сбыта. В 2020 г. установлено местонахождение и ликвидирована подпольная лаборатория, для организации которой участниками преступной группы в Серпуховском районе Московской области приобретен участок земли общей площадью 4 га, на котором ранее располагалось фермерское хозяйство со строениями, в дальнейшем оборудованными для производства наркотиков, их сушки, упаковки и складирования. Имеющееся химическое оборудование позволяло производить до 1,5 тонн наркотических средств в месяц. Сбыт осуществлялся через интернет-магазин, размещенный на торговой площадке «Hydra». Кроме того, продавались прекурсоры и так называ-

[1] График построен на основании данных межведомственной статистической отчетности ГИАЦ МВД России за 2010–2020 гг. (форма № 3-МВ-НОН (173), книга 1).

емые «конструкторы» для производства наркотиков в более мелких лабораториях. Задержаны организаторы наркопроизводства, три химика-технолога и курьер-закладчик, работавшие вахтовым методом. Изъято более 100 кг наркотических средств в кристаллизованной форме, 1,5 т в жидком состоянии, 4 т химических реактивов, 670 кг прекурсоров, семь химических реакторов объемом от 100 до 300 л каждый, а также различное лабораторное оборудование.

Работа на данном направлении организована в рамках распоряжений МВД России от 28 января 2020 г. № 1/758 и от 4 марта 2021 г. № 1/2240 «О предоставлении сведений о фактах выявления нарколабораторий и пресечения незаконного распространения прекурсоров».

ГУНК МВД России организована работа по выявлению новых химических веществ, используемых для незаконного изготовления наркотических средств и психотропных веществ, с целью рассмотрения вопроса об оперативном включении их в Перечень.

В результате принятия Правительством РФ постановлений от 28 марта 2018 г. № 337, от 22 февраля 2019 г. № 182 и от 3 декабря 2020 г. № 2007, разработанных ГУНК МВД России, под контроль поставлены 35 новых прекурсоров.

ГУНК МВД России рассматриваются для включения в качестве прекурсоров в подконтрольные списки Перечня еще 61 новое вещество, используемое наркодельцами для незаконного синтеза наркотиков в подпольных лабораториях. Мониторинг ситуации в сфере оборота прекурсоров и других химических веществ, используемых для наркопроизводства, продолжается.

Наращиваются темпы изъятия прекурсоров и выявления фактов их незаконного оборота. Официальная статистика показывает, что принимаемые в данной области меры имеют положительные результаты.

В 2020 г. прекурсоров изъято более чем в 2 раза больше, чем за последние пять лет (7 т 270 кг, с 2015 по 2019 годы — 3 т 351 кг). В период с 2015 по 2020 г. выявлено более чем в 6 раз больше преступлений, связанных с незаконным оборотом прекурсоров[1].

Так, 30 июля 2020 г. в с. Малое Саврасово Раменского района Московской области в ходе санкционированного обследования дома, арендуемого П., изъято 10 кг смеси, содержащей мефедрон, а также около 1 т прекурсоров.

[1] Статьи 228.3 и 228.4 УК РФ (в 2020 г. зарегистрировано 163 преступления, ответственность за которые предусмотрена ст. 228.3 УК РФ, и 128 преступлений, ответственность за которые установлена ст. 228.4 УК РФ).

В июле 2020 г. в Кемеровской области задержан грузовой автомобиль, из которого изъято свыше 1,5 т различных прекурсоров, предназначенных для незаконного изготовления синтетических наркотиков.

Для применения в практической деятельности ГУНК МВД России совместно с ВИПК МВД России подготовлено и направлено в территориальные органы МВД России научно-практическое пособие «Особенности борьбы с незаконным изготовлением и производством синтетических наркотиков в условиях подпольных лабораторий». В настоящее время совместно с ФКУ «Объединенная редакция МВД России» ведется разработка соответствующего учебного фильма.

22 сентября 2020 г. проведено заседание Государственного антинаркотического комитета[1] (протокол № 46), на котором рассмотрен вопрос о совершенствовании механизма противодействия производству и распространению синтетических наркотиков, в том числе путем установления мер контроля за оборотом веществ, используемых для их изготовления.

Во исполнение принятого на заседании ГАК решения (п. 1.1) разработан механизм (путем включения мероприятий в межведомственный план) обмена информацией относительно ввозимых химических веществ, не находящихся под контролем на территории РФ, с установленным фактом их использования для незаконного изготовления наркотических средств, психотропных веществ и их прекурсоров.

В 2021 г. создана межведомственная рабочая группа ГАК по всестороннему изучению проблемных вопросов, связанных с оборотом синтетических наркотиков и веществ, используемых для их производства. Межведомственной группой определены перечень и количество лабораторного оборудования и неподконтрольных веществ, которые могут быть использованы для незаконного производства наркотических средств, психотропных веществ и их прекурсоров в условиях подпольных лабораторий. Изучается возможность установления мер контроля при реализации такого оборудования и веществ физическим лицам.

В рамках межведомственной рабочей группы ГАК прорабатывается возможность установления размеров (объемов) разрешенных для приобретения, перевозки и хранения физическими лицами прекурсоров таблиц II и III списка IV Перечня, для личного использо-

[1] Далее — ГАК.

вания, за исключением прекурсоров, являющихся лекарственными средствами.

Минпромторгом России совместно с МВД России во исполнение решения ГАК (п. 1.3) разрабатываются новые стандартные образцы наркотических средств, психотропных веществ и их прекурсоров для обеспечения экспертно-криминалистических подразделений.

Во исполнение решения ГАК (п. 1.5) Минобрнауки России совместно с Минпромторгом и МВД России прорабатывается возможность организации дополнительных обучающих семинаров для сотрудников полиции по знаниям в области органической химии и соблюдению мер личной безопасности при работе с используемыми наркопроизводителями опасными для жизни и здоровья химикатами.

Для дополнительного стимулирования сотрудников оперативных подразделений, осуществляющих противодействие наркопреступности, в том числе в сфере борьбы с наркопроизводством, ГУНК МВД России разработан приказ МВД России от 13 мая 2020 г. № 279[1], которым для них установлена надбавка к должностному окладу за выполнение задач, непосредственно связанных с риском (повышенной опасностью) для жизни и здоровья в мирное время.

С 1 января 2021 г. ГУНК МВД России на основе последних актуальных тенденций наркоситуации подготовлена и введена новая ведомственная система оценки подразделений наркоконтроля МВД России[2], в которой введены дополнительные критерии оценки: количество выявленных преступлений, связанных с незаконным производством наркотиков, и преступлений, предусмотренных ст. 228.3 и 228.4 УК РФ, в расчете от штатной численности подразделений наркоконтроля территориального органа МВД России.

---

[1] О внесении изменений в приказ МВД России от 21 мая 2018 г. № 314 «О размерах надбавки к должностному окладу сотрудников органов внутренних дел Российской Федерации за выполнение задач, непосредственно связанных с риском (повышенной опасностью) для жизни и здоровья в мирное время, и утверждении Перечня должностей сотрудников органов внутренних дел Российской Федерации, при замещении которых устанавливается надбавка к должностному окладу за выполнение задач, непосредственно связанных с риском (повышенной опасностью) для жизни и здоровья в мирное время».

[2] Распоряжение от 27 ноября 2020 г. № 1/13346 «Об утверждении системы изучения и оценки эффективности деятельности подразделений по контролю за оборотом наркотиков территориальных органов МВД России на региональном уровне».

Негативные тенденции, связанные с ростом нелегального наркопроизводства, находятся в центре внимания государства. Неслучайно уничтожение инфраструктуры незаконных производства, транспортировки и распространения наркотиков, существенное сокращение сырьевой базы незаконного производства наркотиков на территории Российской Федерации остаются в числе основных стратегических задач Стратегии государственной антинаркотической политики Российской Федерации до 2030 года[1].

Обеспечение совершенствования методов выявления, предупреждения и пресечения деятельности организованных групп и преступных сообществ (преступных организаций), осуществляющих изготовление наркотических средств и психотропных веществ в условиях подпольных лабораторий, предусмотрено и п. 24 межведомственного плана по реализации Стратегии на период 2021–2023 гг.

Президентом Российской Федерации В.В. Путиным на расширенном заседании коллегии МВД России 3 марта 2021 г. еще раз была обозначена необходимость «...и дальше последовательно ликвидировать подпольные производства наркотических средств и каналы наркотрафика».

---

[1] Пункт «д» ст. 11 Стратегии антинаркотической политики Российской Федерации на период до 2030 года, утвержденной Указом Президента РФ от 23 ноября 2020 г. № 733; далее — Стратегия.

Р.Г. Искалиев, А.В. Телков

Современное состояние оперативно-розыскного противодействия преступлениям экономической и коррупционной направленности с использованием информационно-коммуникационных технологий

Анализ правоприменительной практики показывает, что подавляющее большинство криминальных деяний, совершенных с применением ИКТ, носят имущественный характер, в том числе мошенничества, предусмотренные ст. 159, 159.3, 159.6 УК РФ.

В 2019 г. проблемы, возникающие в области противодействия ИКТ-преступности, были рассмотрены на заседании коллегии МВД России (решение от 1 ноября 2019 г. № 3км), в результате чего в оперативных и следственных подразделениях центрального аппарата и территориальных органах МВД России созданы структурные подразделения, специализирующиеся на противодействии преступлениям данного вида. На сегодняшний день их штатная численность составляет около 5 тыс. единиц.

Специализированные IT-подразделения созданы и в подразделениях экономической безопасности и противодействия коррупции (далее — ЭБиПК), которые занимаются выявлением, предупреждением, пресечением и раскрытием преступлений экономической и коррупционной направленности, многие из которых совершаются с использованием ИКТ.

Говоря об имеющихся тенденциях, следует отметить, что в целом на долю IT-подразделений службы ЭБиПК приходится, может, и не самое большое количество киберпреступлений, но, на наш взгляд, наиболее вредоносные как для государства, так и для граждан. Среди них: финансовые интернет-пирамиды, фальшивомонетничество, незаконные азартные игры в сети, осуществление противоправных сделок с использованием криптовалют, попытки махинаций с электронными цифровыми подписями.

По итогам 2020 г. IT-отделения и группы в структуре подразделений ЭБиПК общей численностью 236 единиц выявили 1243 киберпреступления, или 8% от общего числа таких противоправных

деяний, что в целом соотносится с долей экономических преступлений (15 742) от общего числа зарегистрированных IT-составов.

Наибольшее количество криминальных деяний данной категории задокументировано подразделениями ИКТ ЭБиПК ГУ МВД России по г. Москве (620), МВД по Республике Татарстан (141), ГУ МВД России по Новосибирской (51), Московской (40) областям, Ставропольскому краю (38), Кемеровской (33), Волгоградской (30) областям.

Материальный ущерб в размере 581,1 млн руб., задокументированный указанными подразделениями, возмещен на 60,2% (349,7 млн руб.).

ИКТ активно применяются злоумышленниками в сфере незаконной организации и проведения азартных игр. В 2020 г. выявлено 696 преступлений, предусмотренных ст. 171.2 УК РФ, из них 59 преступлений совершены в крупном и особо крупном размере. В суд направлены уголовные дела о 363 преступлениях. Выявлено 1,1 тыс. лиц, совершивших преступления, из них 694 привлечены к уголовной ответственности.

Так, в результате комплекса ОРМ подразделениями ЭБиПК пресечена деятельность преступного сообщества под руководством четырех граждан, которые в сети подпольных игорных заведений на территории г. Москвы, Челябинской области и других субъектов Российской Федерации в период с мая 2018 г. по январь 2019 г. организовали проведение азартных игр вне игорных зон с использованием информационно-телекоммуникационной сети Интернет. В преступное сообщество входили самостоятельные структурные подразделения со строгой иерархией и четким распределением роли каждого участника, которым использовались различные способы конспирации, включая наличие системы допуска к проводимым незаконным азартным играм. По данному факту СУ СК России по Челябинской области 31 января 2020 г. возбуждено уголовное дело в отношении четырех организаторов преступного сообщества по ч. 1 ст. 210 УК РФ и в отношении 15 его активных участников по ч. 2 ст. 210 УК РФ.

В результате комплекса ОРМ пресечена деятельность организованной группы, осуществлявшей противоправную деятельность на территории ряда регионов Российской Федерации. Участники группы из числа руководителей ООО «Букмекер Паб» в период 2017–2019 гг. на территории Брянской области, действуя умышленно, из личной заинтересованности, не исполнили обязанности налогового агента по перечислению в бюджетную систему Российской Федерации исчисленных и удержанных налогов на до-

ходы физических лиц (НДФЛ), полученных от участия в азартных играх, проводимых в букмекерской конторе и тотализаторе, в особо крупном размере на общую сумму 200,5 млн руб. По данному факту СУ СК России по Брянской области 24 апреля 2020 г. возбуждено уголовное дело по ч. 2 ст. 199.1 УК РФ.

В 2020 г. ГУЭБиПК МВД России совместно с МВД по Республике Татарстан пресечена деятельность преступного сообщества, члены которого занимались изготовлением и реализацией на территории различных регионов Российской Федерации поддельных билетов Банка России номиналом 2 тыс. руб. посредством интернет-площадки «HYDRA».

В Мурманской области по материалам сотрудников IT-подразделения регионального УЭБиПК 31 марта 2020 г. возбуждено шесть уголовных дел по ч. 1 ст. 187 УК РФ в отношении группы лиц, направивших от имени руководителей ряда коммерческих организаций, использовав ключи электронных цифровых подписей последних, поддельные платежные поручения о переводе денежных средств на общую сумму более 26,4 млн руб.

Несмотря на имеющиеся положительные результаты ОРД в данной сфере, по нашему мнению, существует целый комплекс проблем правового, методического, организационного характера, создающий трудности для противодействия преступлениям в сфере ИТТ.

Значительную сложность представляет установление личности преступника, совершившего преступление на территории иностранного государства либо зарегистрировавшего «противоправный» интернет-домен в компании, представительство которой находится за рубежом, а также использующего для совершения противоправных действий мессенджеры *Telegram*, *Instagram*, *Viber*, *WhatsApp*, *Skype*, *Jabber*, *Black-Jack*. В своей работе они применяют технологии шифрования, а серверы расположены за пределами Российской Федерации. Помимо того, что значимые сведения могут быть получены только при направлении запроса о правовой помощи в компетентные органы иностранного государства, разрешение которого требует значительного периода времени, законодательство иностранного государства может допускать анонимность пользователя сети Интернет в тех случаях, в которых российское законодательство ее исключает.

Иным способом сохранения преступником конфиденциальности в сети Интернет является использование SIM-карт, приобретенных с нарушением законодательства (например, у граждан, продающих ранее купленные для собственных нужд SIM-карты, или у органи-

заций, закупивших идентификационные модули абонентов якобы для своих сотрудников и в дальнейшем перепродающих их без надлежащего оформления).

На фоне правовой неопределенности статуса криптовалют и стремительного развития криминального «крипторынка» возрастает количество фактов использования денежных суррогатов при совершении преступлений в сфере экономики, уклонения от уплаты налогов, финансирования экстремистской и террористической деятельности.

Определенные шаги на пути совершенствования мер по противодействию ИКТ-преступлениям уже сделаны законодателем.

Так, Федеральным законом от 30 декабря 2020 г. № 533-ФЗ «О внесении изменений в Федеральный закон “О связи”» внесены изменения, касающиеся порядка заключения, прекращения договоров об оказании услуг связи и внесения в них изменений дистанционным способом. Теперь усилены требования к дистанционным продажам SIM-карт, для осуществления которых необходима усиленная квалифицированная электронная подпись или простая электронная подпись, полученная при личной явке за оказанием государственных и муниципальных услуг в электронной форме. Кроме того, при использовании простой электронной подписи гражданам необходимо пройти идентификацию через Единую биометрическую систему (ЕБС), оператором которой является Ростелеком.

Принят Федеральный закон от 31 июля 2020 г. № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации», устанавливающий правила выпуска цифровых финансовых активов, оборота цифровой валюты (криптовалюты). Запрещено принимать оплату товаров, работ и услуг цифровой валютой, она признана имуществом.

Развитие ведомственных информационно-аналитических ресурсов, обеспечивающих деятельность МВД России, в том числе в части обеспечения экономической безопасности, на наш взгляд, является одним из приоритетных направлений деятельности ОВД Российской Федерации.

В настоящее время в МВД России эксплуатируются следующие информационные ресурсы, обеспечивающие экономическую безопасность:

- сервис обеспечения экономической безопасности ОВД Российской Федерации предназначен для обеспечения полного технологического цикла ввода, накопления, обработки и ана-

лиза оперативно-служебной, аналитической и оперативно-розыскной информации в ГУЭБиПК МВД России, а также в подразделениях ЭБиПК территориальных органов МВД России на региональном уровне. Использование сервиса повышает качество работ по выявлению, предупреждению, пресечению и раскрытию преступлений экономической и коррупционной направленности;

- информационно-поисковый сервис «Следопыт-М» предназначен для поиска, сбора, обработки и представления информации, получаемой из разнородных информационных систем и баз данных, используемых в оперативных подразделениях на федеральном, межрегиональном, региональном и территориальном уровнях системы МВД России. ИПС «Следопыт-М» призван повысить эффективность информационного обеспечения деятельности подразделений оперативно-розыскной информации МВД России за счет сокращения времени и трудозатрат при получении информации, содержащейся в ИС и БД, путем формирования единого поискового запроса, сбора, обработки информации, досье в рамках унифицированного интерфейса и статистической отчетности.

В соответствии с п. 8 Перечня поручений по реализации Послания Президента Российской Федерации Федеральному Собранию Российской Федерации от 20 февраля 2019 г. № Пр-294 (далее — Перечень) МВД России совместно с заинтересованными органами государственной власти и организациями обеспечено внедрение цифровой платформы для приема обращений субъектов предпринимательской деятельности в связи с оказанием на них давления со стороны правоохранительных органов. Организовано обеспечение МВД России технической возможностью приема обращений с цифровой платформы, структурных подразделений центрального аппарата МВД России — технической возможностью направления уведомлений об окончании их рассмотрения на цифровую платформу в соответствии с п. 2 распоряжения МВД России от 9 сентября 2019 г. № 1/10132, регламентирующего порядок рассмотрения обращений, поступивших с цифровой платформы. Во исполнение п. 9 Перечня МВД России издано распоряжение от 9 сентября 2019 г. № 1/10132, предусматривающее порядок рассмотрения обращений, поступивших с цифровой платформы для приема обращений субъектов предпринимательской деятельности в связи с оказанием на них давления со стороны правоохранительных органов, функционирование которой обеспечивается ав-

тономной некоммерческой организацией «Платформа для работы с обращениями предпринимателей».

Контроль за рассмотрением каждого обращения поручен руководителям структурных подразделений центрального аппарата МВД России. Уведомления об окончании рассмотрения обращений будут направляться на цифровую платформу для использования в целях, предусмотренных уставом автономной некоммерческой организации «Платформа для работы с обращениями предпринимателей».

16 сентября 2019 г. об исполнении п. 9 Перечня поручений доложено Президенту Российской Федерации В.В. Путину.

Кроме того, МВД России осуществляет централизованное информационное обеспечение в установленном порядке подразделений МВД России, органов государственной власти Российской Федерации, правоохранительных органов иных государств оперативно-справочными, оперативными, розыскными, криминалистическими, дактилоскопическими, статистическими, архивными и научно-техническими сведениями.

Основными проблемными вопросами при организации противодействия преступлениям экономической и коррупционной направленности, совершенным с использованием ИТТ, по-прежнему являются:

— длительные сроки получения информации от кредитных организаций, операторов связи, социальных сетей и компаний, предоставляющих интернет-услуги;

— использование преступниками при совершении преступлений широкого спектра средств сокрытия личности (анонимные телефонные карты, VPN-сервисы, анонимные браузеры, IP-телефония);

— недостаточная квалификация сотрудников специализированных оперативных подразделений.

Существенно ограничивает возможности расследования указанных видов преступлений недостаточное программно-техническое обеспечение производства компьютерных экспертиз. Так, при проведении экспертиз, объектами которых являются заблокированные мобильные телефоны и планшеты, имеющие графические или неизвестные цифровые пароли, доступ к внутренней памяти устройств можно получить только в отдельных случаях (в зависимости от модели, операционной системы, серии чипсетов). Помимо этого, эксперты сталкиваются с проблемой шифрования самой внутренней памяти мобильных устройств.

По нашему мнению, ограниченные возможности по производству компьютерно-технических экспертиз и длительное время их проведения приводят к тому, что органы предварительного следствия не назначают соответствующие экспертизы (и не предъявляют обвинения по дополнительным эпизодам преступной деятельности), в связи с чем часть преступлений в сфере ИТТ может оставаться без должного реагирования, а права потерпевших — без защиты.

Несмотря на осуществляемые мероприятия по совершенствованию информационного обмена в сфере противодействия ИКТ-преступности, одной из основных проблем остается недостаточный уровень организации взаимодействия ОВД с кредитными организациями, интернет-провайдерами, операторами сотовой связи и интернет-сервисов.

Особого внимания заслуживает необходимость упрощения порядка получения информации от оператора связи о телефонных соединениях и информации от кредитно-финансовых организаций о принадлежности счета и движении по нему денежных средств.

Прогнозируя развитие ОРД подразделений ЭБиПК в условиях пандемии, можно ожидать рост обращений граждан и организаций (экономической направленности), касающихся нарушения процедур закупок, завышения стоимости лекарственных препаратов и средств индивидуальной защиты, хищения бюджетных денежных средств, выделенных на борьбу с коронавирусной инфекцией COVID-19, преступлений в сфере производства и потребительского рынка, мошенничеств в сети Интернет, а также мошенничеств, связанных с налоговой, банковской, коммерческой и иной деятельностью, которые характеризуются гибкой адаптацией к новым формам и методам предпринимательской деятельности, имитацией заключения договоров и осуществления гражданско-правовых сделок.

Исходя из изложенного, на наш взгляд, необходимо проделать значительный объем организационной работы, чтобы обеспечить своевременное реагирование на возрастающие угрозы в рассматриваемой сфере, а именно:

- закрепить возможность ограничения доступа (блокирования) к сайтам интернет-пирамид (хайп-проектам);
- законодательно закрепить возможность «исследования компьютерной информации», полученной в результате ОРМ, в том числе с привлечением квалифицированных специалистов, обладающих специальными знаниями, т.е. фиксации юридически значимых следов киберпреступлений в интернете;

- организовать для борьбы с ИКТ-преступлениями единый электронный документооборот с кредитными организациями, интернет-провайдерами и операторами связи;
- провести разработку обобщенных методик документирования таких преступлений и обеспечить их распространение в подразделения ЭБиПК территориальных ОВД в целях оказания методической помощи специализированным оперативным подразделениям на основе анализа наиболее значимых преступлений;
- проводить учебные занятия с руководителями и сотрудниками подразделений ИТТ ЭБиПК территориальных ОВД в целях совершенствования организации их деятельности и повышения уровня профессиональной подготовки;
- организовать и провести комплекс оперативно-профилактических мероприятий с целью информирования физических и юридических лиц о способах совершения преступлений с использованием ИКТ, применяемых для этого злоумышленниками методах и средствах, мерах по противодействию этим попыткам, с привлечением для этих целей СМИ, органов государственной власти и местного самоуправления, общественных организаций и других институтов гражданского общества.

А.В. Телков

К вопросу об использовании информационно-коммуникационных технологий для защиты бюджетных средств, выделяемых на реализацию национальных проектов (программ)

В целях осуществления прорывного научно-технологического и социально-экономического развития Российской Федерации, увеличения численности населения, повышения уровня жизни граждан, создания комфортных условий для их проживания, а также условий и возможностей для самореализации и раскрытия таланта каждого человека в соответствии с Указом Президента РФ от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» утверждены национальные проекты (программы) по следующим направлениям:

- демография;
- здравоохранение;
- образование;
- жилье и городская среда;
- экология;
- безопасные и качественные автомобильные дороги;
- производительность труда и поддержка занятости;
- наука;
- цифровая экономика;
- культура;
- малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы;
- международная кооперация и экспорт;
- а также Комплексный план модернизации и расширения магистральной инфраструктуры.

На реализацию указанных национальных проектов (программ) до 2024 г. планируется выделить 25,7 трлн руб., из которых более 13 трлн руб. — из федерального бюджета, почти 5 трлн руб. — из бюджета субъектов РФ, около 150 млрд руб. — из средств госу-

дарственных внебюджетных фондов, более 7,5 трлн руб. — из внебюджетных источников.

По предварительным данным Министерства финансов Российской Федерации, исполнение расходов федерального бюджета на нацпроекты за 2020 г. составило 97,4%, или 2,149 трлн руб. Лидерами по исполнению расходов на 1 января 2021 г. являются нацпроекты «Жилье и городская среда» — 99,7% и «Наука» — 99,2%, а также Комплексный план модернизации и расширения магистральной инфраструктуры (транспортная часть) — 99,4%. Кроме того, в части исполнения расходов наиболее эффективными проектами стали нацпроекты «Безопасные и качественные автомобильные дороги» — 98,8%, «Производительность труда и поддержка занятости» — 98,7%, «Культура» — 98,5%, «Демография» — 98%, «Международная кооперация и экспорт» — 97,6% и «Экология» — 97,6%[1].

Одним из приоритетных направлений деятельности государства в целом и ОВД в частности является защита этих средств от преступных посягательств.

МВД России во взаимодействии с другими правоохранительными и контролирующими органами на постоянной основе проводит комплекс мероприятий, направленных на выявление, пресечение и раскрытие преступлений экономической и коррупционной направленности в сфере защиты бюджетных средств, выделяемых на финансирование национальных проектов (программ), направленных на реализацию Указа Президента РФ от 7 мая 2018 г. № 204.

В результате проведенных мероприятий в 2020 г. органами внутренних дел выявлено 1,9 тыс. преступлений, связанных с освоением бюджетных средств. Почти каждое второе преступление (более 1,3 тыс.) квалифицировалось как совершенное в крупном и особо крупном размере либо причинившее крупный ущерб, 61 преступление — как совершенное в составе организованной группы или преступного сообщества. Установлено более 1,1 тыс. лиц, совершивших данные преступления, из них в отношении 0,8 тыс. лиц уголовные дела направлены в суд. Совокупный материальный ущерб, причиненный этими преступлениями, составил 18,2 млрд руб., при этом 10,8 млрд руб. возмещены государству.

[1] Минфин сообщил, что бюджет на нацпроекты в 2020 году исполнен на 97,4% // ТАСС. URL: https://tass.ru/nacionalnye-proekty/10493091 (дата обращения: 01.02.2021).

По сведениям ФКУ «ГИАЦ МВД России», в 2020 г. органами внутренних дел проведена 7851[1] проверка физических и юридических лиц, получивших средства федерального бюджета (из них юридических лиц — 6389), направленные на реализацию национальных проектов (программ). По ее результатам выявлено 660 нарушений, 473 — совершенных юридическими лицами, 187 — физическими лицами. При таком количестве проведенных проверок выявлено всего 466 преступлений (5,9%), из которых:

— по национальному проекту «Демография» — 141 преступление;

— национальному проекту «Образование» — 94 преступления;

— национальному проекту «Жилье и городская среда» — 75 преступлений;

— национальному проекту «Здравоохранение» — 47 преступлений;

— национальному проекту «Экология» — 25 преступлений;

— национальному проекту «Культура» — 13 преступлений;

— национальному проекту «Малое и среднее предпринимательство и поддержка индивидуальной предпринимательской инициативы» — 21 преступление;

— национальному проекту «Безопасные и качественные автомобильные дороги» — 32 преступления;

— национальному проекту «Производительность труда и поддержка занятости» — 1 преступление;

— национальному проекту «Цифровая экономика» — 2 преступления;

— национальному проекту «Наука» — 3 преступления;

— национальному проекту «Международная кооперация и экспорт» — 1 преступление;

— по Комплексному плану модернизации и расширения магистральной инфраструктуры — 11 преступлений.

Анализ имеющихся материалов проверок и уголовных дел в данной сфере позволяет сделать вывод о том, что в настоящее время посягательства на бюджетные средства в большинстве случаев осуществляются путем необоснованного увеличения цен на материально-технические ценности и оказываемые услуги, а также завышения объемов выполненных работ, в том числе с использованием служебного положения должностными лицами органов власти и управления, имеющими отношение к выделению, распределению и освоению бюджетных средств.

[1] По данным ФКУ «ГИАЦ МВД России», форма «Нацпроект» (465), книга 1.

Статистические данные убедительно свидетельствуют о том, что наибольшее количество расследуемых в органах предварительного следствия МВД России преступлений коррупционной направленности приходится на деяния, совершенные против собственности, среди которых самым распространенным является мошенничество (ч. 3 и 4 ст. 159 УК РФ).

На наш взгляд, сложности в выявлении преступлений в сфере реализации национальных проектов обусловлены тем обстоятельством, что бюджетные средства расходуются в основной своей части на проведение строительно-ремонтных работ, проверки полноты выполнения которых сопряжены с проведением долгосрочных, трудоемких и дорогостоящих экспертиз (исследований). Проверки расходования бюджетных средств, выделенных на информатизацию различных отраслей экономики, обусловливают необходимость привлечения узкоспециализированных специалистов в области компьютерных технологий, которых также проблематично привлечь в ходе доследственной проверки. Необходимо отметить тот факт, что имеющиеся в большинстве регионов страны специалисты ведомственных экспертных учреждений (МВД России и Минюста России) не способны в полной мере удовлетворить все потребности подразделений ЭБиПК, что негативно отражается на результатах работы по выявлению и раскрытию преступлений в бюджетной сфере.

В 2020 г. наиболее типичными являлись расследуемые факты хищений бюджетных средств, связанные с предоставлением руководителями коммерческих организаций подложных сведений об оказании образовательных услуг, реализуемых в рамках федерального проекта «Старшее поколение» национального проекта «Демография», завышением объемов и стоимости произведенных работ при выполнении государственных и муниципальных контрактов, заключенных в рамках реализации национальных проектов «Жилье и городская среда» и «Образование».

Анализ правоприменительной практики свидетельствует о том, что при реализации национальных проектов и государственных программ наиболее криминализованной является сфера закупок. Причем противоправные действия совершаются как представителями организаций, участвующих в закупках в качестве потенциальных исполнителей контрактов, так и должностными лицами органов государственной власти и местного самоуправления, а также подведомственных им организаций и учреждений.

Одним из способов совершения противоправных деяний является заключение картельных соглашений, не позволяющих другим участникам торгов снижать цену контракта и одерживать победу на аукционах на право заключения государственного контракта.

Так, в результате совместной с Управлением «П» СЭБ ФСБ России, УФСБ России по Воронежской области и УЭБиПК ГУ МВД России по Воронежской области реализации оперативных материалов СЧ по РОПД ГСУ ГУ МВД России по Воронежской области 22 января 2020 г. возбуждено уголовное дело по ч. 3 ст. 30 и ч 2 ст. 178 УК РФ в отношении учредителя ООО «Комстрой», представителя ООО «Икс Телеком», соучредителя ООО «СКС Пром», представителя ООО «АКС ГРУПП», представителя АО ФИРМА «СМУР» и по ч. 5 ст. 33, ч. 3 ст. 30, ч. 2 ст. 178 УК РФ в отношении заместителя директора Департамента организации строительства централизованных проектов Макрорегионального филиала «Центр» ПАО «Ростелеком», которые в результате заключения между хозяйствующими субъектами — конкурентами соглашений, запрещенных в соответствии с антимонопольным законодательством, обеспечивающих видимость конкурентной борьбы и поддержания максимально высокой цены контракта, заключили договоры, в том числе на строительство линий связи при реализации федерального проекта «Информационная инфраструктура» национальной программы «Цифровая экономика Российской Федерации» на общую сумму более 965 млн руб., где незаконная прибыль составила бы 778 млн руб.

На наш взгляд, в целях выявления картельных сговоров необходимо проводить оперативно-розыскные мероприятия, направленные на установление фактического местонахождения IP-адресов, с которых подавались заявки на электронные площадки. Отправление заявок и предложений с IP-адресов, находящихся по одному почтовому адресу, может свидетельствовать об аффилированности участвующих в торгах лиц и наличии ограничивающих конкуренцию соглашений.

По мнению автора, расследование несвоевременно выявленных коррупционных преступлений в бюджетной сфере, когда проведение оперативно-розыскных мероприятий уже не актуально, а доказательственная база, которая могла бы содержаться на электронных или материальных носителях, уничтожена, сопряжено со значительными сложностями в доказывании. Проблемы выявления и расследования данной категории преступлений, как правило, обусловлены способами подготовки к совершению преступления и действиями по сокрытию его следов. Так, полномочия

по подписанию документов делегируются неаффилированным подставным лицам; принятие решения или выражение согласия на подписание документов осуществляется коллегиально; взятки маскируются под законные платежи; вместо передачи денежных средств оплачиваются услуги; взятки передаются третьими лицами, не имеющими очевидных связей с взяткодателем или взяткополучателем, наличными или выплачиваются из специальных «фондов» (slush funds), не вовлеченных непосредственно в преступную схему. Кроме того, доказывание преступного умысла на совершение коррупционного преступления осложняют способы коммуникации преступников. Зачастую удаленное общение организуется через защищенные мессенджеры с шифрованием, во время встреч используются сообщения, написанные от руки или напечатанные на электронном устройстве, а сами встречи проводятся в местах, оговоренных злоумышленниками ранее (до попадания в орбиту внимания правоохранительных органов), а также на территориях ограниченного доступа или за границей.

При таких приемах противодействия со стороны лиц, совершающих противоправные действия, правоохранителям необходимо активнее использовать современные приемы и средства получения компьютерной информации, мониторинг сети Интернет, проводить сложные оперативно-розыскные мероприятия, ограничивающие конституционные права и свободы человека и гражданина, такие как снятие информации с технических каналов связи, получение компьютерной информации.

Одним из распространенных способов хищения бюджетных средств является их вывод через цепочку аффилированных организаций за рубеж. В последнее время для легализации (отмывания) доходов, полученных преступным путем, все чаще используются различные виртуальные активы, в том числе криптовалюта. В связи с этим особое значение для защиты средств бюджета, выделяемых на реализацию национальных проектов (программ), приобретает применение информационно-коммуникационных технологий. Вывод денежных средств за рубеж осуществляется, как правило, путем заключения мнимых внешнеэкономических сделок, в том числе с использованием фирм-однодневок, выявление которых возможно с использованием программного сервиса АСК НДС-3, находящегося на вооружении у налоговых органов.

Данный программный комплекс позволяет полностью автоматизировать процесс контроля за движением средств между счетами юридических и физических лиц и повысить его продуктивность с 10 до 100%. Алгоритм интеллектуального поиска дает возмож-

ность автоматически выстраивать цепочки движения денежных средств между юридическими и физическими лицами и видеть, в числе прочего, уплачен ли налог на добавленную стоимость в этих цепочках. Принцип работы сервиса заключается в том, что программа сверяет все имеющиеся у нее данные между декларациями, книгами покупок и книгами продаж разных категорий налогоплательщиков, выявляя при этом цепочки контрагентов. Если имеются расхождения, программа автоматически формирует требование налогоплательщику о представлении пояснений по выявленным расхождениям. Такой сервис позволяет бороться с «фирмами-однодневками». С 2018 г. в базу АСК НДС-3 добавлена база кредитных учреждений, что также усовершенствовало новый сервис ФНС России для поиска незаконных вычетов НДС. При этом сервис АСК НДС-3 анализирует движение денежных средств не только между компаниями и индивидуальными предпринимателями, но и между компаниями и физическими лицами. Сервис АСК НДС-3 также обрабатывает данные кассовых аппаратов и сверяет их с книгами продаж. После запуска сервиса АСК НДС-3 государство вышло на новый уровень борьбы с «фирмами-однодневками», а также противодействия иным способам обналичивания денежных средств. При организации эффективного внешнего взаимодействия правоохранительные органы России могут использовать данный сервис в оперативных интересах, в том числе и для противодействия хищениям бюджетных средств.

С мая 2019 г. ГУЭБиПК МВД России использует возможности подсистемы управления национальными проектами ГИИС «Электронный бюджет» (ведется Минфином России), которая позволяет осуществлять контроль эффективности расходования бюджетных средств в режиме реального времени. Подключение ответственных сотрудников подразделений ЭБиПК к данному сервису позволяет проводить поисковые мероприятия, направленные на получение оперативно значимой информации, не выходя из кабинета.

В феврале 2021 г. стало известно о создании Федеральной службой по финансовому мониторингу (Росфинмониторинг) сервиса под названием «Прозрачный блокчейн», позволяющего отслеживать криптовалютные операции россиян. О запуске этой системы глава ведомства Юрий Чиханчин рассказал на встрече с президентом России Владимиром Путиным. По словам Ю.А. Чиханчина, «Прозрачный блокчейн» позволит «увидеть все движения с криптовалютой, то есть попытки спрятаться за криптовалюту». Он также отметил, что сервис уже начал работу, по результатам которой «есть уголовные дела». Глава Росфинмониторинга сообщил,

что ведомство работает в области мониторинга криптовалютных транзакций при содействии коллег из других стран, включая Финляндию, Люксембург, Лихтенштейн, Белоруссию и Мальту. Контроль за данным проектом осуществляет Правительство при участии Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации[1].

Таким образом, в случае использования криптовалюты для легализации денежных средств, выделенных на реализацию национальных проектов и похищенных из бюджета, применение технологии «Прозрачный блокчейн», основанной на анализе криптовалютных транзакций с помощью искусственного интеллекта, позволит устанавливать лиц, участвующих в незаконных схемах по хищению бюджетных средств и их легализации.

В ходе мониторинга реализации национальных и федеральных проектов ГУЭБиПК МВД России выявлены проблемы отсутствия достаточных ресурсов на проведение строительно-технических экспертиз и ряда других востребованных правоохранительными органами экспертиз (товароведческих, правовых), а также системы аттестации экспертов и аккредитации экспертных организаций, имеющих право на проведение экспертиз документов, используемых в области закупок телекоммуникационного и программного обеспечения, в том числе иностранного производства. Данная проблема озвучена Министром внутренних дел РФ В.А. Колокольцевым на заседании президиума Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам под председательством Председателя Правительства РФ М.В. Мишустина от 28 февраля 2020 г. № 2. Вместе с тем в протоколе заседания отражен вопрос проведения экспертиз документов, используемых в области закупок телекоммуникационного и программного обеспечения, в том числе иностранного производства. В связи с этим МВД России в Минцифры России направлены предложения относительно создания системы аттестации экспертов и аккредитации экспертных организаций, имеющих право на проведение экспертиз документов, используемых в области закупок телекоммуникационного и программного обеспечения, в том числе иностранного производства. В соответствии с поручением Заместителя Председателя Правительства РФ Д.Н. Чернышенко от 2 сентября 2020 г. № ДЧ-П10–10321 в Минцифры России в состав межве-

[1] Встреча с директором Федеральной службы по финансовому мониторингу Юрием Чиханчиным // Официальный сайт Президента России. URL: http://www.kremlin.ru/events/president/news/65036 (дата обращения: 07.04.2021).

домственной рабочей группы по сертификации экспертов и оценке соответствия экспертных учреждений для производства экспертиз в сфере информационно-коммуникационных технологий, методическому обеспечению и производству экспертиз в указанной сфере включен сотрудник МВД России.

В дальнейшем начальник ГУЭБиПК МВД России 20 мая и 5 октября 2020 г. принял участие в выездных совещаниях Секретаря Совета Безопасности Российской Федерации по вопросам «О дополнительных мерах по противодействию правонарушениям в ходе реализации национальных проектов в субъектах Российской Федерации, находящихся в пределах Приволжского федерального округа» и «О дополнительных мерах по противодействию правонарушениям в ходе реализации национальных проектов в субъектах Российской Федерации, находящихся в пределах Сибирского федерального округа», а также 9 декабря 2020 г. в заседании Координационного совещания руководителей правоохранительных органов Российской Федерации по вопросу «О результатах работы правоохранительных органов Российской Федерации по противодействию коррупции, в том числе в рамках Национального плана противодействия коррупции на 2018–2020 годы, утвержденного Указом Президента РФ от 29 июня 2018 г. № 378».

В рамках указанных совещаний обсуждался ряд проблем, препятствующих надлежащему выполнению поставленных задач:

— о необходимости заключения органами исполнительной власти субъектов Российской Федерации соглашений с Росфинмониторингом об организациях, участвующих в реализации национальных проектов, имеющих риски неисполнения обязательств по госконтрактам (риск-ориентированный подход), которые позволят превентивно реагировать на негативные проявления со стороны недобросовестных подрядчиков и минимизировать факты хищения бюджетных средств;

— целесообразности совершенствования полномочий руководителей субъектов при распределении финансов при расходовании средств на внезапно возникающие нужды;

— своевременном получении информации от органов исполнительной власти субъектов Российской Федерации о рисках нецелевого расходования и несвоевременного доведения средств, предусмотренных на реализацию национальных и федеральных проектов, а также об иных нарушениях, возникающих в ходе реализации проектов.

Таким образом, в целях повышения эффективности противодействия преступлениям, связанным с неправомерным использованием денежных средств, выделенных из бюджетов всех уровней

на реализацию национальных проектов, федеральных целевых программ, государственных программ субъектов Российской Федерации и муниципальных программ, руководителям территориальных подразделений ЭБиПК целесообразно:

- организовать систему оперативного отслеживания бюджетных средств — от главного распорядителя до конечного получателя с учетом региональной специфики и объемов бюджетного финансирования, в том числе обеспечить оперативным сотрудникам доступ к подсистеме управления национальными проектами ГИИС «Электронный бюджет», которая позволяет осуществлять контроль эффективности расходования бюджетных средств в режиме реального времени;
- проводить оценку коррупционных рисков в сфере закупок для государственных (муниципальных) нужд и закупок отдельными видами юридических лиц, устанавливать угрозы и уязвимости, требующие повышенного внимания правоохранительных органов (внедрение риск-ориентированного подхода при выявлении и расследовании коррупционных преступлений, совершаемых в ходе закупочной деятельности), что позволит своевременно реагировать на складывающуюся оперативную обстановку в данной сфере. Суть этого подхода заключается в выявлении возможно проблемных организаций, для которых характерен ряд признаков (например: совершение подозрительных финансовых операций, в том числе до заключения госконтракта; отсутствие собственного капитала; малочисленность персонала и др.);
- внедрить и активно использовать проект «Личный кабинет правоохранительного органа», который позволит всем территориальным подразделениям МВД России оперативно получать в электронном виде информацию о финансовых рисках по всей стране;
- создавать специализированные подразделения по проведению экспертиз в рамках контроля за реализацией национальных проектов;
- учитывать при планировании ОРМ характеристики организаций, непосредственно осваивающих бюджетные средства, выделенные на реализацию национальных проектов, включение их в реестр недобросовестных поставщиков, в том числе используя информационные ресурсы, имеющиеся в Росфинмониторинге, Федеральной антимонопольной службе и налоговых органах; устанавливать их аффилированность должностным лицам, курирующим те или иные региональные программы (проекты), а также причастность к хищениям бюджетных средств и их последующей легализации.

П.В. Эзрохин

Цифровые технологии в оперативно-розыскной деятельности уголовного розыска по противодействию организованной преступности

Необходимость повышения эффективности и результативности противодействия организованной преступности обусловливает переориентацию подразделений уголовного розыска (УР) ОВД с автономных ОРМ на комплексное использование сил и средств, в том числе для разоблачения организованных преступных групп (ОПГ) и преступных сообществ (ПС) в сети Интернет и киберпространстве, результатом чего должно стать пресечение организованной преступной деятельности банд, ОПГ и ПС этнической направленности, а также организованных преступных структур террористического и экстремистского характера, обладающих международными и транснациональными связями.

Современный этап эволюционирования организованной преступности в Российской Федерации (с 2008 г. по настоящее время) характеризуется попытками повторного передела сфер влияния в криминальном мире. Говоря о современной организованной преступности, необходимо отметить, что на ее состояние негативно влияют освобождающиеся из мест лишения свободы осужденные на рубеже 90-х гг. прошлого века к длительным срокам заключения бывшие участники так называемых организованных ПС (в Москве и Московской области — «солнцевские», «ореховские», «бауманские», «подольские», «люберецкие», в Санкт- Петербурге и Ленинградской области — «тамбовские», «малышевские», в Татарстане — «тяп-ляп», «жилплощадка», на Дальнем Востоке — ОПГ «Общак», в Рязанской области — «слоны» и т.д.).

Современная российская организованная преступность представляет собой гибридный тип, сформированный из участников региональных и местных ОПГ и ПС общеуголовной и экономической направленности, специализирующихся как на традиционных преступлениях — вымогательстве (рэкете), разбойных нападениях, криминальном автобизнесе, незаконном обороте оружия, наркотиков, организации занятия проституцией, так и на совершении

квалифицированных разбойных нападений с применением огнестрельного оружия на объекты кредитно-финансовой сферы, краж банкоматов с использованием взрывчатых веществ и взрывных устройств, хищений автомашин с применением современных технологий, средств визуального и технического контроля, организации незаконной миграции, а также различных видах преступлений общеуголовной и экономической направленности с использованием сферы высоких информационных технологий[1], в интернет-сети и киберпространстве.

Важными научными задачами ОРД являются системный анализ правовых основ и законодательных норм, регламентирующих данный вид деятельности, равно как и порядка ведомственно-правовой регламентации вопросов организации и тактики проведения ОРМ, а также выявление новых частных закономерностей оперативно-розыскной практики и их обоснование.

В частности, анализируя тенденции преступной деятельности ОПГ и ПС за последние 10 лет, нельзя не отметить закономерную связь между характером преступлений на почве экстремизма, международными факторами, влияющими на их распространение, и переходом организованной преступности в пространство информационных технологий с целью использования сознания людей для их вовлечения в экстремистско-террористическую деятельность, приобретающую организованный характер[2].

В процессе оперативно-розыскного противодействия организованной преступности важное значение приобретает взаимодействие подразделений УР с другими оперативными подразделениями ОВД, правоохранительных ведомств и правоохранительных органов зарубежных государств, в результате которого можно получать информацию о деятельности террористических организаций и экстремистских сообществ: по распространению экстремистских материалов (публичные призывы к осуществлению экстремистской деятельности, публичное оправдание терроризма и др.); по скло-

---

[1] См.: *Эзрохин П.В.* Совершенствование правовых и организационных основ оперативно-розыскной деятельности подразделений уголовного розыска по противодействию организованной преступности: монография / ФГКУ ДПО «ВИПК МВД России». Домодедово, 2018. С. 45.

[2] См.: Статистические сборники ГИАЦ МВД России и результаты оперативно-служебной деятельности органов внутренних дел (2015–2019 гг.); Аналитический обзор результатов анкетирования сотрудников подразделений уголовного розыска органов внутренних дел, специализирующихся на противодействии организованной преступности / ГУ МВД России по Московской области. М., 2018.

нению, вербовке или иному вовлечению лиц в совершение преступлений террористической и экстремистской направленности, руководству сообществом, организацией и его частью; разработке планов и условий для совершения преступлений террористической и экстремистской направленности; инструктажу участников форумов; сбору денег для поддержки экстремистских движений; созданию сайтов, содержащих сведения о лицах, поддерживающих экстремизм, публикации на них данных о времени и встрече заинтересованных лиц; использованию интернета для информационно-психологического воздействия, обращений к массовой аудитории с сообщениями о будущих и уже спланированных экстремистских действиях и террористических акциях; рассылке подобных сообщений по электронной почте; вовлечению в совершение деяний новых лиц, у которых нет умысла на совершение преступлений террористической и экстремистской направленности, но которые своими действиями способствуют их совершению. Причем оперативно-розыскные действия и такие ОРМ, как оперативный поиск, наведение справок, опрос, наблюдение, оперативное внедрение, отождествление личности, можно осуществлять в виртуальном пространстве, используя такие методы ОРД, как легендирование, аналитическая разведка, разведывательный опрос и др.

Таким образом, использование методов и средств ОРД по противодействию современной организованной преступности в виртуальном пространстве сети Интернет следует рассматривать как оперативно-розыскную тактику по разоблачению преступной деятельности банд, ОПГ и ПС, в том числе террористического и экстремистского характера.

Исследование проблем организационного и методического обеспечения противодействия организованной преступности подразделениями УР неразрывно связано с изучением особенностей применения оперативно-розыскных методик выявления и раскрытия оперативными подразделениями ОВД преступлений, совершенных участниками и лидерами банд, ОПГ и ПС в современных условиях.

Под методом в науке следует понимать способ анализа действительности, способ изучения, исследования явлений природы и общества. Методологией принято называть учение о методе, способе исследования или совокупность приемов, методов исследования, применяемых в какой-либо науке[1]. В свою очередь, полагаем, что методика представляет собой алгоритм, процедуру для проведения

[1] См.: Краткий философский словарь / под ред. М. Розенталя и П. Юдина. М.: Гос. изд-во политич. лит-ры, 1955. С. 283, 285.

каких-либо целенаправленных действий. Методика отличается от метода конкретизацией приемов и задач. Все это относится и к применению оперативно-розыскных методик противодействия организованной преступности подразделениями УР.

Исходными элементами оперативно-розыскной методики являются: знание субъектами ОРД способов совершения конкретных видов преступлений; использование оперативно-розыскных мер для выявления лиц, занимающихся преступной деятельностью; получение сведений о механизме образования ОПГ и ПС, типологии поведения их участников и лидеров, а также сведений виктимологии.

Совокупность этих и других знаний позволяет принимать организационно-тактические решения:

— о необходимости применения ОРМ;

— приоритетности тех или иных гласных и негласных мер;

— применении оперативно-технических средств и тактических приемов осуществления ОРМ.

Важность разработки и совершенствования системы оперативно-розыскных методик по противодействию организованной преступности подразделениями УР в современных условиях также обусловлена приспособлением криминальной среды к реалиям складывающейся оперативной обстановки, использованием участниками и лидерами банд, ОПГ и ПС сферы высоких технологий, выходом в сеть Интернет, налаживанием международных и транснациональных связей с участниками организованных преступных структур зарубежных государств, повышением уровня финансового, технического и технологического обеспечения организованной преступной деятельности, использованием современных систем связи, аудио-, видеонаблюдения и контрнаблюдения.

Вне всяких сомнений, подразделения УР столкнулись с такой формой организованной преступности, как этнической, методы противодействия которой были утрачены в связи с реорганизацией системы борьбы с организованной преступностью, что существенно повлияло на результативность повседневной оперативной работы подразделений УР в данном направлении.

В связи с этим, *во-первых*, с целью решения данной проблемы требуется глубокая научно-методическая проработка организации ОРД в сфере противодействия подразделениями УР этнической организованной преступности. Без ее кардинального реформирования и создания полноценного аппарата конфидентов, способных решать стратегические и тактические задачи в сфере противодействия организованной преступности мигрантов общеуголовной

направленности, невозможно будет сформировать стратегические позиции, отвечающие реалиям времени, чтобы противостоять инновационным формам организованной преступной деятельности в условиях современности.

Во-вторых, научно-методической проработки в соответствии с перспективами совершенствования негласной работы в сфере противодействия организованной преступности требует организация применения негласных форм и методов в телекоммуникационных системах и сети Интернет, что, безусловно, актуализируется в связи с развитием информационных технологий. Выход организованной преступности в киберпространство, а также использование участниками и лидерами банд, ОПГ и ПС, в том числе экстремистской и террористической направленности, информационного поля, а также высоких технологий при подготовке и совершении тяжких и особо тяжких преступлений заставляют сотрудников подразделений УР отходить от годами выработанных стереотипов формирования ОРД.

Стремительное развитие информационных технологий приводит к тому, что многие явления социальной жизни все в большей мере находят отражение в так называемых «виртуальных мирах», т.е. информационных средах, носителями которых выступают как СМИ, так и глобальные компьютерные телекоммуникационные сети и системы.

В силу того, что организованная преступность в настоящее время оказывает возрастающее влияние на самые разные стороны социальной, экономической и политической жизни общества, борьба с ней должна предусматривать применение всех возможных средств и методов. Эта борьба естественным образом должна охватывать «информационные сферы», которые включают в себя в первую очередь СМИ, а также средства телекоммуникаций и связи, глобальные компьютерные сети, индустрию самых разнообразных информационных услуг.

Применение современных информационных технологий привело к формированию принципиально новых направлений в деятельности органов внутренних дел в рамках борьбы как с организованной преступностью, так и с преступностью в сфере высоких технологий[1].

В самом общем плане **аналитическую разведку** можно определить как «разведку в информационной среде» и в то же время как

[1] См.: *Овчинский С.С.*, *Овчинский А.С.*, *Овчинский В.С.* Оперативно-розыскная информация: монография. 2-е изд., доп. М.: ИНФРА-М, 2017. С. 316, 319.

«получение новых знаний о разведываемом объекте или явлении на основании аналитической обработки добытой разведывательной информации и сведений об известных фактах». Аналитическая разведка включает в себя изучение материалов скрытого наблюдения, оперативных установок, сообщений негласных сотрудников, данных перехвата с различных каналов связи, а также анализ сообщений, публикаций и выступлений в средствах массовой информации, статистических данных, сведений, которые содержатся в государственных и негосударственных автоматизированных банках данных и информационных системах. Аналитическая разведка открывает новые возможности для решения задач борьбы с организованной преступностью, во-первых, в силу возможности использования сотен электронных банков данных, содержащих самые разнообразные сведения, и, во-вторых, в связи с совершенствованием эффективных методов обработки различной информации, использование которой позволяет решать задачи в сфере борьбы с организованной преступностью.

Сущность **компьютерной разведки** заключается в поиске и получении информации из компьютерных систем и сетей. Осуществляется компьютерная разведка с помощью аппаратно-программных компьютерных средств, путем применения логических операций и приемов. Компьютерная разведка является одним из наиболее эффективных средств профилактики, противодействия и борьбы с самыми разнообразными компьютерными преступлениями, поскольку в задачи компьютерной разведки входит и поиск злоумышленников в компьютерных сетях. В правовом отношении компьютерную разведку можно рассматривать как разновидность таких ОРМ, как снятие информации с технических каналов связи, наблюдение, исследование предметов и документов, оперативный осмотр[1] и получение компьютерной информации.

Обеспечение информационной безопасности формируется из практики применения средств специальной техники в ОРД. В настоящее время применение технических средств в отношении организованной преступности переходит в сферу информационно-технического противодействия. Использование в преступной деятельности современных средств коммуникации, в свою очередь, открывает новые возможности для получения ценной оперативно значимой информации и документирования преступных действий путем скрытого контроля сообщений, передаваемых с помощью

[1] См.: *Овчинский С.С.*, *Овчинский А.С.*, *Овчинский В.С.* Оперативно-розыскная информация: монография. 2-е изд., доп. М.: ИНФРА-М, 2017. С. 328.

различных систем связи. Таким образом, борьба с организованной преступностью, переходя в информационно-техническую сферу, должна предусматривать и операции по скрытому выявлению, контролю, а в ряде случаев и по блокированию работы и выводу из строя нелегальных радиосетей, развернутых ОПГ и ПС.

Информационно-психологические воздействия, как осознаваемые, так и неосознаваемые, могут быть узконаправленными — выборочными, нацеленными на конкретных людей. Для таких воздействий могут быть использованы электронные СМИ, компьютерные сети, видео-, аудио- и программные продукты. Эти аппаратно-программные комплексы, которые являются отголосками фундаментальных проектов по созданию психотропного оружия, используют эффект так называемого 25-го кадра.

В процессе неосознаваемых воздействий информация, невидимая глазом с экрана монитора, входит в подсознание человека, обходя защитные функции мозга и вызывая или изменение реакций испытуемого в случае тестирования, или целенаправленные действия в случае его зомбирования.

В целом перед правоохранительными органами стоит задача создания мультимедийных компьютерных комплексов информационно-психологических воздействий, которые должны стать необходимым инструментом оперативных комбинаций и следственных действий[1].

Одним из наиболее перспективных направлений совершенствования информационно-аналитического обеспечения ОРД подразделений УР по противодействию организованной преступности является создание в сетевом пространстве негласно контролируемых **легендированных объектов**, которые представляют определенный интерес для установления лиц, использующих интернет в преступных целях. Ими могут являться создаваемые в оперативных целях интернет-компании и сайты-ловушки, размещаемые на сетевых ресурсах, которые осуществляют свою деятельность под контролем сотрудников подразделений УР. Такого рода легендированные объекты могут создаваться в рамках организации и проведения оперативного эксперимента, оперативного внедрения, наведения справок, получения компьютерной информации и других ОРМ для пресечения преступной деятельности ОПГ, в том числе экстремистского и террористического характера.

[1] См.: *Овчинский С.С.*, *Овчинский А.С.*, *Овчинский В.С.* Оперативно-розыскная информация: монография. 2-е изд., доп. М.: ИНФРА-М, 2017. С. 326.

Легендированные объекты в сетевой среде интернета могут быть двух типов:

1) объекты, непосредственно созданные оперативными подразделениями ОВД для решения оперативных задач;

2) объекты, созданные физическими и юридическими лицами, которые согласны использовать их в интересах оперативных подразделений ОВД в сфере противодействия организованной преступности.

Одним из тактических приемов доступа к оперативно значимой информации в сетевом пространстве для разоблачения преступной деятельности ОПГ и ПС является оперативное внедрение — легендированный ввод конфидента в сетевую криминальную среду или закрытые криминогенные объекты сетевого общения. При этом оперативное внедрение в закрытые форумы и чаты должно осуществляться по правилам внедрения в ОПГ и ПС с учетом возможностей проверки участниками организованных преступных структур внедряемого лица.

К наиболее эффективным тактическим приемам ОРД подразделений УР по противодействию организованной преступности относится оперативное внедрение негласных источников в сетевую криминальную среду или закрытые объекты сетевого общения в целях выявления преступлений террористической направленности и пресечения преступной деятельности транснациональных ОПГ и ПС. Тактика оперативного внедрения в таких случаях не выходит за рамки приемов, используемых для проведения подобного рода ОРМ. В частности, осуществляется подбор конфидентов из активных пользователей сетей или разрабатываемых лиц; проводится их проверка, выявляются наличие у них оперативных возможностей и умение работать в сетевом общении с лицами, имеющими криминальные устремления. Оперативное внедрение в закрытые форумы и чаты должно осуществляться по правилам подготовки и проведения ОРМ «оперативное внедрение».

Таким образом, полагаем, что использование в качестве тактического приема оперативного внедрения в сети Интернет может стать наиболее перспективной формой противодействия транснациональным ОПГ и ПС, в том числе в сфере незаконного оборота оружия, нелегальной миграции, а также религиозного и международного экстремизма.

Анализ правовых основ межгосударственной нормативно-правовой базы в сфере противодействия организованной преступности на уровне Совета Министров внутренних дел государств — участников СНГ показывает, что в данной области ОРД требуется вне-

сение изменений и дополнений. В число нормативных правовых актов, нуждающихся в доработке и повышении качества их практического применения для решения стратегических и тактических задач противодействия организованной преступности, в том числе транснационального и террористического характера, входят:

— Соглашение о сотрудничестве министерств внутренних дел в сфере борьбы с организованной преступностью (Ашхабад, 16–17 февраля 1994 г.);

— Решение о проекте Положения о Бюро по координации борьбы с организованной преступностью и иными опасными видами преступлений на территории государств — участников СНГ (БКБОП) (Минск, 30–31 января 2002 г., Москва, 25 ноября 2005 г.);

— Решение о Специализированном банке данных БКБОП (Санкт-Петербург, 17 сентября 2010 г.);

— Решение об утверждении Инструкции о порядке функционирования Специализированного банка данных БКБОП (Минск, 2 сентября 2015 г., 6 сентября 2016 г.).

Необходимость внесения изменений и дополнений в отдельные положения этих документов, на наш взгляд, обусловлена отставанием заложенных в них правовых норм от складывающейся оперативной обстановки в сфере противодействия организованной преступности. Например, ст. 2 Соглашения о сотрудничестве министерств внутренних дел в сфере борьбы с организованной преступностью, принятого в Ашхабаде 16–17 февраля 1994 г., определены формы сотрудничества в борьбе с организованной преступностью, к числу которых отнесен и обмен информацией о различных событиях и фактах, представляющих оперативный интерес для решения задач противодействия организованной преступности.

Вместе с тем в данной статье Соглашения не предусмотрен какой-либо обмен информацией между компетентными органами министерств внутренних дел стран — участниц Содружества Независимых Государств по вопросам предоставления сведений об участниках и лидерах ОПГ и ПС экстремистской и террористической направленности, формах и способах подготовки и совершения ими преступлений, а также использования сети Интернет, новых видов информационных технологий и киберпространства для обсуждения подготовки и совершения экстремистских и террористических акций на родном языке. Такой обмен информацией осуществляется лишь через БКБОП в порядке, установленном нормативными правовыми актами.

Исходя из изложенного выше разработка нового типового Соглашения или корректировка действующих норм, которые бы регламентировали обмен информацией между компетентными органами министерств внутренних дел государств — участников СНГ относительно участников и лидеров ОПГ и ПС экстремистской и террористической направленности, а также формах и способах подготовки и совершения преступлений и использования сети Интернет, новых видов информационных технологий и киберпространства для подготовки, совершения преступлений и сокрытия следов от организованной преступной деятельности, существенно повысили бы качество взаимодействия подразделений УР ОВД как самостоятельного субъекта ОРД в вопросах противодействия организованной преступности, в том числе террористического, транснационального и международного характера.

Таким образом, необходимо дополнить ст. 2 Соглашения о сотрудничестве министерств внутренних дел в сфере борьбы с организованной преступностью, принятого в Ашхабаде 16–17 февраля 1994 г., текстом следующего содержания: «обмен информацией между компетентными органами министерств внутренних дел государств — участников СНГ относительно участников и лидеров ОПГ и ПС экстремистской и террористической направленности, а также формах и способах подготовки и совершения преступлений и использования сети Интернет, новых видов информационных технологий и киберпространства для подготовки, совершения преступлений и сокрытия следов от организованной преступной деятельности».

Кроме того, решением от 2 сентября 2015 г. об утверждении Инструкции о порядке функционирования Специализированного банка данных БКОП предусмотрен порядок обмена информацией между ОВД Российской Федерации и зарубежных государств по вопросам противодействия организованной преступности. Приложением № 1 данного документа утвержден типовой формуляр сообщения «организованная преступность». Вместе с тем при создании структуры информационного сообщения не учтен ряд аспектов, что негативно влияет на получение полной информации об объектах учета в сфере противодействия организованной преступности. Так, в структуре сообщения «организованная преступность» отсутствуют сведения об ОПГ и ПС в сфере информационных технологий, что затрудняет обмен оперативными данными между правоохранительными органами зарубежных государств по информационному обеспечению противодействия организованной преступности и не позволяет сформировать банки данных

на ОПГ и ПС, специализирующиеся в данной сфере, в связи с чем необходимо внесение соответствующих дополнений в нормативную базу.

Для достижения значимых результатов в разоблачении преступной деятельности межрегиональных, международных и транснациональных ОПГ и ПС подразделения УР должны обеспечивать эффективное взаимодействие с компетентными органами зарубежных государств, исходя из общей концепции развития международных связей и укрепления сферы международного сотрудничества.

В связи с этим наиболее важное значение международное сотрудничество подразделений УР ОВД с правоохранительными органами зарубежных государств приобретает в сфере противодействия международному наркобизнесу, а также в области пресечения преступной деятельности межрегиональных, международных и транснациональных ОПГ и ПС террористической и экстремистской направленности, нелегальной иммиграции, противодействия незаконному обороту оружия и торговле людьми, а также противодействия организованной преступности в сфере высоких информационных и IT-технологий, в том числе в киберпространстве с использованием ИИ.

* * *

Что касается проблематики концептуальной модели противодействия транснациональной организованной преступности, то необходимо отметить, что ее разработка должна осуществляться путем международно-правового сотрудничества на уровне государства и его правоохранительных органов, где в качестве основной идеи должна превалировать стратегия всеобщей безопасности, а уже потом реализовываться основные национальные интересы в сфере охраны порядка. Следует подчеркнуть, что с учетом роста проявлений организованной преступности мигрантов и ее террористической составляющей, увеличения в структуре организованной преступности количества преступлений, совершенных с применением оружия, использования транснациональными ОПГ и ПС международных связей, а также использования современных информационных технологий, в том числе IT-технологий и интернет-пространства, как никогда важным является установление связей между подразделениями УР России и правоохранительными органами иностранных государств.

А.В. Воронцов

К вопросу об использовании данных, полученных в ходе оперативно-розыскной деятельности органов внутренних дел в сети Интернет, в борьбе с организованной преступностью

Стратегией национальной безопасности Российской Федерации[1] одной из основных угроз государственной и общественной безопасности признана деятельность организованных преступных групп и преступных сообществ (далее — ОПГ и ПС). Получение и использование информации об участниках и связях ОПГ и ПС, размещенной в сети Интернет, в ОРД ОВД РФ регламентированы рядом нормативных правовых актов[2].

Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» предоставляет сотрудникам полиции право использовать в работе информационные системы, вести видеобанки и видеотеки лиц, проходивших (проходящих) по делам и материалам проверок, формировать, вести и использовать банки данных оперативно-справочной, криминалистической, розыскной и иной информации о лицах, предметах и фактах, использовать банки данных других государственных органов и организаций, в том числе персональные данные граждан[3].

ФЗ об ОРД предоставляет субъектам ОРД право создавать и использовать информационные системы[4]. В 2016 г. перечень ОРМ был дополнен ОРМ «получение компьютерной информации»[5].

---

1 Утверждена Указом Президента РФ от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации».

2 Федеральные законы от 12 августа 1995 г. № 144-ФЗ «Об оперативно-розыскной деятельности», от 7 июля 2003 г. № 126-ФЗ «О связи», от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 г. № 152-ФЗ «О персональных данных», от 7 февраля 2011 г. № 3-ФЗ «О полиции».

3 Пункт 33 ст. 13 Федерального закона «О полиции».

4 Статьи 6, 10 Федерального закона «Об оперативно-розыскной деятельности».

5 Статья 3 Федерального закона от 6 июля 2016 г. № 374-ФЗ «О внесении изменений в Федеральный закон “О противодействии терроризму” и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности».

В соответствии с прим. 1 к ст. 272 УК РФ компьютерная информация — это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Компьютерная информация имеет следующие юридически определяемые формы представления: сетевой адрес, доменное имя, файл, электронная подпись, электронное сообщение, электронный документ, программа для ЭВМ, база данных, информационная система, сайт в сети Интернет, страница сайта в сети Интернет, электронный журнал, электронные денежные средства[1].

Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» (далее — Закон о связи) установил основания для ограничения тайны связи, обязанности операторов связи и процедуру ограничения прав пользователей услугами связи при проведении ОРМ. Согласно ч. 2 ст. 64 Закона о связи операторы связи обязаны обеспечивать реализацию установленных Министерством связи и массовых коммуникаций РФ по согласованию с государственными органами, осуществляющими ОРД или обеспечение безопасности Российской Федерации, требований к сетям и средствам связи для проведения этими органами ОРМ в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий[2].

Согласно ст. 64 Закона о связи и п. 14–15 Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, утвержденных постановлением Правительства РФ от 27 августа 2005 г. № 538, операторы связи — юридические лица или индивидуальные предприниматели, оказывающие услуги связи на территории РФ, обязаны хранить и предоставлять в установленном законом порядке государственным органам, осуществляющим ОРД:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи, в том числе:

— фамилию, имя, отчество, место жительства и реквизиты основного документа, удостоверяющего личность абонента-гражданина;

---

[1] *Вехов В.Б., Васюков В.Ф.* Получение компьютерной информации от организаторов ее распространения в сети Интернет при расследовании преступлений // Российский следователь. 2018. № 3 (СПС «КонсультантПлюс»).

[2] Статья 64 Федерального закона «О связи».

— наименование юридического лица, его место нахождения, а также список лиц, использующих оконечное оборудование юридического лица, в котором указаны их фамилии, имена, отчества, места жительства и реквизиты основных документов, удостоверяющих личность;

— сведения баз данных о расчетах за оказанные услуги связи, в том числе о соединениях, трафике и платежах абонентов;

— сведения об абонентских номерах, которые сохраняются абонентами при заключении договоров об оказании услуг связи с другими операторами подвижной радиотелефонной связи, и наименования указанных операторов;

2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео-, иные сообщений пользователей услугами связи.

Во исполнение п. 1 ст. 64 Закона о связи были подготовлены Правила хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи, утвержденные постановлением Правительства РФ от 12 апреля 2018 г. № 445, которые определили порядок, сроки и объем хранения операторами связи текстовых сообщений пользователей услугами связи, голосовой информации, изображений, звуков, видео- и иных сообщений пользователей услугами связи на территории РФ.

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» определяет понятие информации, регламентирует информацию как объект правовых отношений, устанавливает порядок доступа к различным видам информации, регулирует сферу применения информационных технологий, создания и использования информационных систем и информационно-телекоммуникационных сетей. В соответствии со ст. 10.1 указанного Закона организаторы распространения информации в сети Интернет — лица, осуществляющие деятельность по обеспечению функционирования информационных систем и (или) программ для ЭВМ, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети Интернет, обязаны хранить на территории РФ и представлять в установленном законом порядке уполномоченным государственным органам, осуществляющим ОРД или обеспечение безопасности Российской Федерации:

- информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети Интернет и информацию об этих пользователях в течение одного года с момента окончания осуществления таких действий;
- текстовые сообщения пользователей сети Интернет, голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети Интернет до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Во исполнение ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» были разработаны Правила взаимодействия организаторов распространения информации в информационно-телекоммуникационной сети Интернет с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, утвержденные постановлением Правительства РФ от 31 июля 2014 г. № 743, и Правила хранения организаторами распространения информации в информационно-телекоммуникационной сети Интернет информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей информационно-телекоммуникационной сети Интернет и информации об этих пользователях, предоставления ее уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность или обеспечение безопасности Российской Федерации, утвержденные постановлением Правительства РФ от 31 июля 2014 г. № 759. Последними был определен состав информации, подлежащей хранению организатором распространения информации в сети Интернет при обеспечении функционирования коммуникационного интернет-сервиса (далее — КИС):

1) сведения о пользователе, в том числе идентификатор пользователя в КИС;

2) сведения регистрационных данных, включающие в себя:

— информацию о сетевом адресе, с которого осуществлена регистрация пользователя, с указанием точного времени регистрации;

— информацию, внесенную в КИС пользователем или организатором распространения информации в сети Интернет при регистрации пользователя;

— информацию, автоматически передаваемую в ходе регистрации КИС в силу используемых сетевых протоколов с помощью установленных на устройстве пользователя программ для ЭВМ;

— информацию, фактически фиксируемую КИС при регистрации пользователя с использованием иных КИС;

3) сведения о фактах авторизации, включающие в себя:

— информацию о фактах авторизации пользователя с указанием его идентификатора в КИС, точного времени и сетевых адресов, с которых осуществлялась авторизация;

— информацию, фактически фиксируемую КИС при авторизации пользователя с использованием авторизации в иных КИС;

— информацию, автоматически передаваемую в ходе авторизации КИС в силу используемых сетевых протоколов с помощью установленных на устройстве пользователя программ для ЭВМ;

4) информацию об изменениях либо о дополнении пользователем информации о номере телефона или адресе электронной почты, а также иных сведений, указанных им при регистрации;

5) информацию об оказанных организатором распространения информации в сети Интернет платных услугах пользователю с указанием точного времени их оказания, организации, оказывающей платежную услугу, а также фактически фиксируемой КИС информации об оплате таких услуг (валюта, сумма, номер транзакции, использованная платежная система и идентификаторы платежной системы);

6) информацию о факте прекращения регистрации в КИС с указанием идентификатора пользователя в КИС, точного времени и сетевых адресов, с которых осуществлялось прекращение регистрации;

7) фактически фиксируемую КИС информацию о пользователях в случае, если КИС предоставляет возможность приема, передачи и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователям сети Интернет без регистрации и авторизации;

8) сведения о фактах приема, передачи и (или) обработки голосовой информации, письменного текста, изображений, звуков или иных электронных сообщений пользователей сети Интернет (информация о точном времени приема, передачи, доставки и (или) обработки электронных сообщений с указанием информации об адресатах этих сообщений, в том числе информации для неопределенного круга лиц — пользователей сети Интернет);

9) фактически фиксируемую КИС информацию об организации приема, передачи, доставки и (или) обработки электронных

сообщений, осуществляемых с использованием технологий электронных платежных систем, в том числе информацию о произведенных денежных операциях (с указанием информации о корреспонденте — идентификаторе платежной системы, валюты, суммы, оплачиваемой услуги или товаров (при наличии), об иных данных, указанных при проведении денежной операции), осуществленных транзакциях (с указанием идентификатора платежной системы («электронного кошелька»), суммы прихода либо расхода, иных данных, указанных при осуществлении транзакции).

Во исполнение п. 2 ч. 3 ст. 10.1 Федерального закона «Об информации, информационных технологиях и о защите информации» были подготовлены Правила хранения организатором распространения информации в информационно-телекоммуникационной сети «Интернет» текстовых сообщений пользователей информационно-телекоммуникационной сети Интернет, голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей информационно-телекоммуникационной сети «Интернет», утвержденные постановлением Правительства РФ от 26 июня 2018 г. № 728, которые определили порядок, сроки и объем хранения на территории РФ организатором распространения информации в сети Интернет текстовых сообщений пользователей сети Интернет, голосовой информации, изображений, звуков, видео-, иных электронных сообщений пользователей.

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных» регулирует отношения, связанные с обработкой персональных данных, осуществляемой государственными органами и органами местного самоуправления, юридическими и физическими лицами.

Решением коллегии МВД России от 5 декабря 2018 г. № 2км перед оперативными подразделениями органов внутренних дел РФ была поставлена задача поиска дополнительных источников информации, представляющей интерес в рамках осуществления ОРД[1]. В нашем мире высоких технологий основным источником информации об участниках ОПГ и ПС выступает сеть Интернет. Проведение ОРМ в социальных сетях («ВКонтакте», «Инстаграм», «Одноклассники», «Твиттер», «Фэйсбук» и т.п.) позволяет получить данные:

[1] Приказ МВД России от 18 января 2019 г. № 20 «Об объявлении решения коллегии МВД России от 5 декабря 2018 года № 2км» (п. 15 прил.).

— о структуре и составе ОПГ и ПС;

— местонахождении определенных участников ОПГ и ПС, в том числе скрывающихся под другими данными;

— об их рабочих контактах, преступных и родственных связях;

— используемом конкретными участниками ОПГ и ПС транспорте;

— объектах недвижимости, находящихся во владении, пользовании и распоряжении конкретных участников ОПГ и ПС;

— увлечениях и сексуальных предпочтениях конкретных участников ОПГ и ПС.

Преступность России пронизана множеством внутренних связей. Соучастники ряда преступлений подразделяются на непосредственных исполнителей преступления и их пособников («обслуживающий персонал»). К формам соучастия, которые, как правило, остаются за рамками расследования преступлений, но могут быть установлены через рабочие контакты в сети Интернет, на наш взгляд, относятся:

- кредитование преступной деятельности;
- обеспечение преступным инструментом и технологиями;
- обеспечение преступников различными видами оружия;
- обеспечение фальшивыми документами;
- организация для преступников обезличенной аренды имущества (жилого или служебного помещения, гаража, ангара и т.п.);
- обеспечение преступников транспортом;
- незаконные медицинские услуги (оперирование на дому раненного преступника и т.п.);
- хранение, экспертная оценка и легализация запрещенного законом;
- иные формы криминального соучастия.

Организованная преступность имеет жесткую иерархию — статусные «звания» и «должности». «Звания» начинаются с «бродяги», поднимаются до «авторитета» и «положенца» и заканчиваются «вором в законе», а вот «должности» различаются не по названию («смотрящий»), а в зависимости от масштабов подконтрольного объекта: транспортный узел, район, город, место лишения свободы, субъект РФ.

Сбор информации на специализированных сайтах в сети Интернет, посвященных организованной преступности («КомпроматРу», «МСК1», «ПраймКрайм» и т.п.), поможет получить новые данные о статусе конкретного участника ОПГ и ПС. Полученные данные могут быть использованы в качестве первичной оперативно-розыскной информации, необходимой для расследования уголовных дел и проведения проверок по делам оперативного учета.

Кроме того, участники ОПГ и ПС активно используют являющуюся частью интернета закрытую сеть — Deep Web («темный» или «глубокий» интернет). Сеть Deep Web не индексируется поисковыми системами, что исключает возможность определить, какой информацией обмениваются пользователи. В пространстве «темного» Интернета находятся коммерческие вэб-сайты, торгующие наркотиками, оружием, фальшивыми документами и т.п. В ходе проведения ОРМ в Deep Web можно получить первичную информацию об ОПГ и ПС, совершающих преступления с использованием этой сети.

Таким образом, можно отметить широкие возможности использования в органах внутренних дел РФ данных, полученных в ходе ОРД в сети Интернет, в борьбе с организованной преступностью. Более подробно указанные направления использования данных целесообразно рассмотреть в специализированных журналах МВД России.

В.И. Коваленко

Инновационные технологии в комплексе оперативно-розыскного противодействия торговле людьми

Борьба с торговлей людьми является одним из приоритетных направлений предупредительно-профилактической деятельности российских правоохранительных органов. Решающую роль в выявлении и пресечении указанных посягательств играют оперативные подразделения ОВД. Складывающаяся криминальная ситуация в сфере торговли людьми, устойчивый рост онлайн-посягательств в киберпространстве свидетельствуют о необходимости усиления мер оперативно-розыскного противодействия указанным преступлениям путем применения и использования новых технологических инструментов.

Неблагоприятные тенденции торговли людьми проявляются как в положительной динамике указанных посягательств: по данным ГИАЦ МВД России, темпы прироста торговли людьми (ст. 127.1 УК РФ) в 2020 г. составили 72,7%, было зарегистрировано 38 преступлений; незаконные изготовление и оборот порнографических материалов и предметов (ст. 242 УК РФ) увеличились на 37,6% и составили 1399 преступлений[1], так и в качественной трансформации указанного вида преступности, проявляющейся в стремительной виртуализации, перемещении в информационно-телекоммуникационную сеть Интернет ее наиболее опасных форм — сексуальных посягательств, в том числе сексуального насилия, совершаемых в отношении несовершеннолетних.

Согласно статистическим данным ГИАЦ МВД России в 2020 г. с использованием информационно-телекоммуникационных технологий было совершено 2099 преступлений, связанных с незаконным изготовлением и оборотом порнографических материалов (ст. 242, 242.1, 242.2 УК РФ), общий прирост данной группы посягательств составил 9,6%.

[1] Состояние преступности в России: за январь — декабрь 2020 года / ФКУ «Главный информационно-аналитический центр МВД России» // Официальный сайт МВД России. URL: https://мвд.рф./reports/item/22678184/ (дата обращения: 20.03.2021).

В Генеральной прокуратуре Российской Федерации обращается внимание на резкий рост количества преступлений, совершенных с использованием ИКТ или в сфере компьютерной информации, который в последние годы достиг масштабов, позволяющих говорить об этих деяниях как об угрозе национальной безопасности, особенно с учетом их низкой раскрываемости, фиксируемой на уровне не более 25%. Если еще пять лет назад в общей структуре преступности на долю киберпреступлений приходилось менее 2%, то в 2020 г. они составили уже 25% среди всех преступлений, зарегистрированных в стране, при этом негативная тенденция только усилилась: зафиксированный рост данных посягательств составил 73,4%, а их общее количество за год достигло 510,3 тыс.[1]

Успешной виртуализации/цифровизации преступной деятельности, связанной с торговлей людьми, сексуальной эксплуатацией женщин и детей, трудовой эксплуатацией лиц из уязвимых групп населения (мигрантов, молодежи, пожилых людей), способствовало активное использование преступниками новых технологий вербовки, рекламной деятельности, привлечения и укрытия потенциальных жертв современной работорговли, их последующей эксплуатации и сокрытия следов преступления.

Во время развития пандемии и в постпандемический период активное перемещение в интернет социально-досуговых, служебно-профессиональных и образовательных контактов детей и взрослых предопределило повышенную активность преступников, которые фактически организовали целенаправленную массированную онлайн-атаку на детей и подростков. Опасным последствием деструктивного, особенно сексуализированного, онлайн-общения в сети детей и преступников является назначение последними реальных встреч офлайн с потенциальной жертвой, большая часть из которых заканчивается сексуальным насилием в отношении несовершеннолетнего, на что неоднократно обращалось внимание специалистов[2].

Отмечая серьезную обеспокоенность складывающейся неблагоприятной ситуацией в сфере борьбы с онлайн-формами торговли людьми, *международные эксперты ОБСЕ и Tech Against Trafficking* (далее — ОБСЕ, ТАТ) *подготовили доклад «Использование инно-*

[1] В Генпрокуратуре заявили, что киберпреступность стала представлять угрозу нацбезопасности: по словам представителя ведомства Андрея Некрасова, раскрываемость таких преступлений составляет не более 25%. 2021. 24 мая // ТАСС. URL: https://tass.ru/obschestvo/11451173 (дата обращения: 24.05.2021).

[2] *Жданов Ю., Овчинский В.* Киберполиция XXI века. Международный опыт / под ред. С.К. Кузнецова. М.: Международные отношения, 2020.

ваций в борьбе с торговлей людьми: *комплексный анализ технологических инструментов*», в котором справедливо обращается внимание на то, что борьба с торговлей людьми существенно затруднена из-за постоянного развития бизнес-моделей, используемых торговцами людьми. Авторы доклада подчеркивают, что масштаб торговли людьми исчисляется 24,9 млн жертв во всем мире, поэтому «технологии являются решающим фактором нашего коллективного успеха и должны быть фундаментальным компонентом любой стратегии по борьбе с торговлей людьми»[1].

В связи с этим представляется необходимым более подробно изучить международный опыт применения оперативно-розыскных, научно-технических мер по выявлению, пресечению и предупреждению наиболее распространенных форм торговли людьми, связанных с сексуальными посягательствами в отношении женщин и детей, вербовкой и привлечением потенциальных работников в целях трудовой эксплуатации. Важно знать, какие новые технологии применяют организованные преступные группы зарубежных стран в сфере торговли людьми и какие технологии используются в борьбе с ними.

Соответственно, далее рассмотрим:

1) основные направления использования преступниками информационно-телекоммуникационных технологий, злоупотребление которыми повышает прибыльность преступной деятельности работорговцев в механизме торговли людьми;

2) инновационные технологические инструменты в комплексе мер оперативно-розыскного противодействия указанным посягательствам.

Основные направления использования преступниками ИКТ в механизме торговли людьми

Анализ международной и отечественной правоприменительной практики показывает, что злоупотребление технологиями позволяет преступникам увеличивать размер и прибыльность рынка торговли людьми, превращать уязвимых людей в жертв, осуществлять контроль жертв и оказывать на них влияние, способствовать формированию незаконных финансовых потоков.

Торговля людьми — сложное составное, многоэтапное преступление, механизм совершения которого включает в себя вербовку по-

[1] Бюро Специального представителя и координатора ОБСЕ по борьбе с торговлей людьми и Tech Against Trafficking. Использование инноваций в борьбе с торговлей людьми: комплексный анализ технологических инструментов (Вена, май 2020).

тенциальных жертв, рекламную деятельность, аренду помещений, перевозку жертв, непосредственно саму эксплуатацию жертвы, коммуникации преступников, проведение финансовых расчетов и получение финансовой прибыли от эксплуатации. В эпоху стремительной цифровизации всего общества указанные этапы преступной деятельности, совершаемые с использованием информационно-коммуникационных технологий, оставляют многочисленные, не всегда анонимные, цифровые следы.

Это подтверждается результатами исследований международной практики противодействия современным онлайн-формам работорговли[1]. Эксперты обращают внимание на то, что многие люди, которые сознательно или неосознанно пользуются услугами жертв торговли людьми, прибегают к использованию технологий для доступа, просмотра, записи и распространения информации об этих жертвах. Платформы для такой эксплуатации практически безграничны — социальные сети, онлайн-игры, сайты знакомств, приложения[2].

Новые технологии пронизывают все этапы преступной практики в сфере торговли людьми: вербовку, рекламную деятельность, аренду помещений, перевозку, контроль, принуждение и эксплуатацию жертв, коммуникации и финансовые операции.

Вербовка. Преступники применяют различную тактику для выявления и вербовки (или покупки) жертв торговли людьми в целях их дальнейшей эксплуатации для получения незаконной прибыли или сокращения производственных затрат либо изъятия органов жертв для продажи на нелегальных рынках.

Реклама. Крупные офлайн- или онлайн-платформы используются для размещения рекламы, обзоров, чатов или других форм общения, в частности, для оказания сексуальных услуг, предоставляя секс-торговцам средства для привлечения клиентов и взаимодействия с ними в качестве прелюдии к сексуальной эксплуатации жертв. В случае других форм торговли людьми, например в целях использования принудительного труда или извлечения органов, рекламирование жертв возможно, но обычно происходит на определенных платформах, таких как теневой интернет «Даркнет».

---

[1] См.: Europol, *Situation Report*: *Trafficking in human beings in the EU* (The Hague: Europol, February 2016) [Европол, Ситуационный доклад: Торговля людьми в ЕС (Гаага: Европол, февраль 2016)]. С. 12.

[2] Бюро Специального представителя и координатора ОБСЕ по борьбе с торговлей людьми и Tech Against Trafficking, Использование инноваций в борьбе с торговлей людьми: комплексный анализ технологических инструментов (Вена, май 2020).

В ходе *рекламно-вербовочной* «кампании» преступники ведут активную целенаправленную деятельность, рекрутинг в социальных сетях, блогах, на тематических площадках, рекламируют свой «бизнес» и предлагают участие в нем, дают объявления о кастинге, устраивают интернет-просмотры, тестируют потенциальных жертв на профессиональную пригодность, вплоть до фиксации умений последних на веб-камеру («вебкаминг») в режиме онлайн[1].

Аренда/покупка помещений. Такие помещения необходимы преступникам для укрытия жертв в пути, размещения их в пункте назначения или как места эксплуатации. При *аренде* помещения для использования его в преступных целях также имеют место цифровые следы, поскольку подбор помещения и обсуждение условий аренды в большинстве случаев осуществляются на специализированных сайтах в интернете. Виртуальные площадки и возможность охвата широкой аудитории в сети также значительно снижают финансовые затраты преступников, повышают прибыльность их противоправной деятельности.

Перевозка. Для перевозки своих жертв торговцы людьми могут пользоваться различными услугами. Среди них — оформление проездных документов, законных или фальшивых.

Контроль и принуждение. Жертв принуждают к совершению определенных действий, например, в сфере трудовых отношений или в сфере сексуальных услуг. При этом торговцы людьми контролируют жертв, чтобы те работали по первому требованию и не обращались в правоохранительные органы, НПО или к семье в связи со своей эксплуатацией. Торговцы людьми используют различные методы контроля, включая физическое и психологическое насилие, изоляцию, долговую кабалу, наркотическую зависимость, принуждение, мошенничество, изъятие документов и пр.

Эксплуатация жертв. Жертв эксплуатируют для оказания сексуальных услуг, для выполнения работы, занятия попрошайничеством или совершения преступлений, для извлечения органов и пр. Основная цель преступления — получение торговцами незаконных доходов.

Международные специалисты обращают внимание на то, что значительную долю в онлайн-торговле людьми составляют сексуальные посягательства, совершаемые в отношении несовершеннолетних. Применение технологий играет важную роль в увеличении

---

[1] *Коваленко В.И.* Криминальная эксплуатация человека в России: монография / под ред. д-ра юрид. наук, проф. М.М. Бабаева. М.: Юрлитинформ, 2021.

размера и прибыльности рынка торговли людьми, что может достигаться разными способами. Технологии создают новые «возможности для бизнеса», позволяя предоставлять новые виды «услуг», такие как прямая трансляция сексуальной эксплуатации, в том числе сексуального насилия над детьми, для глобальной аудитории. Они расширяют доступ торговцев людьми к более крупным рынкам и снижают для преступников риск обнаружения и задержания правоохранительными органами.

В эпоху цифрового оформления и сопровождения всех аспектов социальной и профессиональной деятельности населения преступники открыто организуют в сетях фальшивые кадровые агентства, дают объявления о найме работников в самых разных сферах занятости: сиделки, помощницы по хозяйству — в сфере услуг, рабочие в сельскохозяйственной и строительной отраслях, работники швейных производств по пошиву одежды и коммерческих/трудовых артелей по изготовлению товаров массового потребления.

Высокая потребность населения в период пандемии в медикаментах и товарах медицинского назначения предопределила всплеск спроса на услуги работников подпольных лабораторий по производству медицинских товаров (пошив масок, производство и транспортировка антисептических устройств, изготовление медицинских препаратов и т.п.). Очевидно, что сверхвысокая прибыльность такой деятельности обеспечивалась не только за счет низкой себестоимости изготовления несертифицированных медицинских препаратов и товаров, но и за счет низкооплачиваемого или фактически рабского труда завербованных через социальные сети работников, ставших жертвами торговцев людьми, посредством интернет-рекламы.

Коммуникация. Для организации вербовки и эксплуатации жертв применяются различные информационные системы. Они же используются и для контактов, включая установление связи с пользователями товаров или услуг, являющихся результатом торговли людьми. Такие действия, особенно в ходе рекламно-вербовочной деятельности, оставляют вполне очевидные для специалистов цифровые следы.

Финансовые операции. Платежи и переводы денег совершаются на всех перечисленных выше этапах. Помимо осуществления платежей на протяжении всего процесса торговли людьми, торговцы используют прибыль от преступления в своих интересах.

Проведение *финансовых платежей* оставляет цифровые следы, является одним из наиболее ярких маркеров противоправной деятельности, частота которых позволяет судить об интенсивности и масштабе бизнес-индустрии (онлайн-торговли людьми).

Эксперты ООН обращают внимание на то, что независимо от сферы и того места в мире, где работают торговцы людьми, «все они получают выгоду от своей преступной деятельности за счет достижений в области технологий, которые делают транзакции быстрее, проще, дешевле и в конечном итоге более прибыльными»[1]. Ежегодная доходность рассматриваемой преступной деятельности уже в 2014 г. достигала 150 млрд долл.[2]

Одним из наиболее важных и проблемных аспектов злоупотребления технологиями в контексте торговли людьми является то, что они создают новые «возможности для бизнеса», позволяя предоставлять мировой аудитории новые виды «услуг», таких как прямая трансляция половых актов, включая сексуальное насилие над детьми. Этот вид эксплуатации международными экспертами дефинируется как *киберсексуальная торговля*[3].

Кроме того, технологии и цифровизация открыли возможности для производства и коммерциализации порнографии с жертвами торговли людьми в массовом масштабе. Эксплуатация взрослых и надругательство над детьми при личной встрече является общепризнанным преступлением, но технологии позволили злоумышленникам донести это насилие в онлайн-режиме до широкой международной аудитории в обмен на деньги, без личного контакта.

Прямая трансляция также позволяет расширить клиентскую базу: в прошлом торговцы людьми зарабатывали деньги на отдельных лицах или небольших группах покупателей, совершавших транзакции, связанные с эксплуатацией жертвы, при личной встрече, что ограничивало доход, получаемый в каждом случае, но теперь, когда видео сексуальной эксплуатации транслируется

---

1 См.: UN.GIFT, Background Paper, 017 Workshop: *Technology and Human Trafficking. The Vienna Forum to Fight Human Trafficking* (Vienna: UN.GIFT, 13–15 February 2008) [Обзорный документ, Семинар 017: Технологии и торговля людьми. Венский форум по борьбе с торговлей людьми (Вена: UN.GIFT, 13–15 февраля 2008 г.)]. С. 2.

2 Бюро Специального представителя и координатора ОБСЕ по борьбе с торговлей людьми и Tech Against Trafficking. Использование инноваций в борьбе с торговлей людьми: комплексный анализ технологических инструментов (Вена, май 2020).

3 См.: Доклад ОБСЕ, ТАТ.

в прямом эфире, клиентская база может быть намного больше, а прибыль растет в геометрической прогрессии[1].

Зарубежные исследователи подчеркивают, что масштаб такого рода кибербизнеса огромен. Данные о реальном количестве жертв киберсексуальной торговли отсутствуют, но есть сведения о числе детей, ставших жертвами киберсексуальной торговли, в некоторых странах. Так, на Филиппинах, по разным подсчетам, количество случаев киберсексуальной торговли детьми варьируется от 60 тыс.[2] до 1 млн, оборот индустрии сексуального насилия над детьми оценивается в 1 млрд фунтов стерлингов. Оно включает в себя и производство фильмов, содержащих извращения, для британских педофилов, и распространенную услугу «изнасилование напрокат»[3].

В целях повышения эффективности комплексного предупреждения посягательств в сфере торговли людьми в рамках программы предупреждения по результатам *картирования* 305 технологических инициатив, реализованных Tech Against Trafficking (TAT) в сотрудничестве с ОБСЕ, и Глобальной инициативой против транснациональной организованной преступности международными экспертами выделены технологические *меры* (*инструменты*) *реагирования*, которые были классифицированы на 11 категорий в соответствии с их *основными целями*, а именно: 1) выявление жертв / торговцев людьми; 2) повышение осведомленности, образование, сотрудничество; 3) управление цепочками поставок; 4) тенденции в области данных и их картирование; 5) выявление корпоративных рисков; 6) вовлечение работников и расширение их прав

---

1 См.: Europol, *Internet Organised Crime Threat Assessment* (IOCTA) 2018 (The Hague: Europol, 2018) [Европол, Оценка угрозы организованной преступности в Интернете (IOCTA) 2018 (Гаага: Европол, 2018 г.)]. С. 7.

2 См.: Matt Blomberg, "*Global taskforce tackles cybersex child trafficking in the Philippines*" [website] (Reuters, 15 April 2019) [Мэтт Бломберг, «Глобальная целевая группа по борьбе с киберсексуальной торговлей детьми на Филиппинах» [веб-сайт] (Рейтер, 15 апреля 2019 г.)]. URL: www. reuters.com/article/us-philippines-trafficking-children/global-taskforce-tackles-cybersex-child-trafficking-in-the-philippines-idUSKCN1RR1D1 (дата обращения: 08.05.2020).

3 См.: Jon Lockett, "*Rape for rent. Inside Philippines' £1bn 'made to order' child sex abuse industry making sick vids for Brit paedos*" [website] (The Sun, 27 July 2018) [Джон Локетт, «Изнасилование напрокат. На Филиппинах индустрия сексуального насилия над детьми стоимостью 1 млрд фунтов стерлингов производит фильмы, содержащие извращения, для британских педофилов» [веб-сайт] (The Sun, 27 июля 2018 г.)]. URL: www.thesun.co.uk/news/6868807/philippines-child-sex-abuse-vids-brit-paedos/ (дата обращения: 08.05.2020).

и возможностей; 7) кейс-менеджмент по делам жертв и оказание им поддержки; 8) этичные покупки; 9) конфиденциальность/идентичность; 10) безопасность платежей; 11) прочие[1].

Инновационные технологические инструменты в комплексе мер оперативно-розыскного противодействия торговле людьми

Основные категории технологических инструментов противодействия торговле людьми и их назначение определены с учетом следующих целей: обучение по вопросам рисков торговли людьми, обращения за помощью и информирования о потенциальных случаях; устранение возможностей для эксплуатации; выявление жертв; сбор общедоступной информации для борьбы с торговлей людьми; оценка рисков торговли людьми; мониторинг и соблюдение требований; выявление типологий и действия в соответствии с ними. Рассмотрим их подробнее.

Технологии для обучения выявлению и сокращению рисков торговли людьми, обращению за помощью и информированию о потенциальных случаях. Развитие новых технологий, в частности увеличение количества смартфонов, открывает больше возможностей для предоставления и распространения информации *среди групп риска*, *включая мигрантов*. Воспользовавшись этой технологией, несколько организаций применяют накопленные знания и опыт мигрантов для сбора информации посредством краудсорсинга о более безопасных путях миграции и надежных рекрутерах (вербовщиках) и работодателях.

Примеры технических инициатив, разработанных и реализованных для обмена информацией о рисках торговли людьми с работниками или между ними, включают: приложение «Golden Dreams» Института Иссара[2], веб-сайт «Contratados от Centro de los Derechos del Migrante»[3], новый веб-сайт «Migrant Recruitment

---

[1] Бюро Специального представителя и координатора ОБСЕ по борьбе с торговлей людьми и Tech Against Trafficking, Использование инноваций в борьбе с торговлей людьми: комплексный анализ технологических инструментов (Вена, май 2020).

[2] См.: Issara Institute, "*Tech & Innovation empowered worker voice*" [website] (Issara Institute) [Институт Иссара, «Голос сотрудников зазвучал громче, благодаря технологиям и инновациям» [веб-сайт] (Институт Иссара)]. URL: www.issarainstitute.org/issara-labs (дата обращения: 08.05.2020).

[3] См.: Contratados, "*Contratados. Voy Contratado, Voy Informado*" [website] (Centro de los Derechos del Migrante, Inc.) [Contratados, «Contratados». Меня наняли, я проинформирован» [веб-сайт] (Центр по правам мигрантов, Inc.)]. URL: www.contratados.org/en (дата обращения: 08.05.2020).

Adviser» Международного профсоюза[1], «My Labor Matters» («Usaping Trabaho»)[2], приложение «1343 Actionline»[3] и платформа «Pantau Pjtki»[4].

Некоторые из этих инструментов, как, например, приложение «Golden Dreams», разработаны в рамках концепции «работник — работодателю» и предназначены для предоставления глобальным компаниям информации об условиях труда и практике эксплуатации в их цепочках поставок.

Другие инструменты, такие как «Contratados», «Migrant Recruitment Adviser», «My Labor Matters», «1343 Actionline», «Pantau Pjtki», были разработаны как платформы, основанные на концепции «работники — соискателям работы», где работники могут проанализировать своих работодателей и опыт найма в интересах других мигрантов, ищущих работу, и широкой общественности.

Эти технологические ресурсы помогают трудящимся-мигрантам и соискателям работы избежать эксплуататорских схем торговли людьми, знакомят их с правами. Данные технологические средства также могут предоставить работникам возможность конфиденциально сообщать о жалобах и проблемах, повысить прозрачность и ответственность рекрутеров (вербовщиков), а также выявить такие практики, как подмена контрактов, конфискация документов, кража заработной платы, мошенничество и взимание незаконных сборов.

---

1 См.: Recruitment Advisor, "RECRUITMENT ADVISOR. Find the best recruitment agency for your job abroad" [website] (Recrutiment Advisor) [Recruitment Advisor, «RECRUITMENT ADVISOR. Как найти лучшее агентство занятости для работы за рубежом» [веб-сайт] (Recrutiment Advisor)]. URL: www. recruitmentadvisor.org/ (дата обращения: 08.05.2020).

2 См.: Verite, "*My Labor Matters*" [website] (Verite Southeast Asia) [Verite, «Мой труд имеет значение» [веб-сайт] (Verite, Юго-Восточная Азия)]. URL: www.mylabormatters.com/ (дата обращения: 08.05.2020).

3 См.: 1343 Actionline Against Human Trafficking, "*1343 Actionline App*" [website] (Commission on Filipinos Overseas) [1343 Actionline Against Human Trafficking, «Приложение «1343 Actionline» [веб-сайт] (Комиссия по делам филиппинцев за рубежом)]. URL: www.1343actionline.ph/ (дата обращения: 08.05.2020).

4 См.: Tifa Foundation and the Migrant Workers Resource Center, "*Pantau PJTKI*" [website] (the Tifa Foundation and the Migrant Workers Resource Center) [Фонд «Tifa» и Ресурсный центр для трудящихся-мигрантов, «Pantau PJTKI» [веб-сайт] (Фонд «Tifa» и Ресурсный центр для трудящихся-мигрантов)]. URL: www.pantaupjtki.buruhmigran.or.id/ (дата обращения: 08.05.2020).

Примерами более универсальных технологических инструментов, которые позволяют сообщать о подозрительных ситуациях, связанных с торговлей людьми, являются приложения «Stop the Traffik» в США[1], «Trafficking in Trinidad and Tobago»[2], «Rapoto@ Shpeto (Report-Save Life)» в Албании[3] или приложение «Unseen» в Великобритании[4].

Большинство этих приложений содержат инструкции по распознаванию признаков торговли людьми и конфиденциальному сообщению о проблемах. Обычно в приложениях предусмотрены расширенные функции, такие как синхронизация с технологией GPS, которая дает возможность точно указать местоположение обращающейся стороны. Некоторые опции позволяют отправлять изображения и голосовые сообщения.

Онлайн-игры также используются для повышения осведомленности. Это инновационный способ помочь людям, особенно детям и подросткам, узнать больше об этом преступлении в интерактивном режиме. В процессе интерактивной игры пользователи могут познакомиться с различными видами и этапами торговли людьми — от вербовки, эксплуатации и побега из сетей торговцев людьми до восстановления (реабилитации), социальной реинтеграции и борьбы жертв торговли людьми.

Использование видеоигр может быть даже более эффективным в случае просвещения молодежной аудитории в этой сфере. Примеры существующих инициатив с использованием видеоигр

---

1 См.: «Google Play», «*STOP APP*» [веб-сайт] («Stop the Traffik», 10 апреля 2019 г.). URL: www.play.google.com/store/apps/details?id=com.fivestones.fivestones&hl=en (дата обращения: 08.05.2020).

2 См.: «Google Play», «*Trafficking in Trinbago*» [веб-сайт] (Адриан Александер, 28 июля 2016 г.). URL: www.play.google.com/store/apps/details?id=com.ima5.fantastic.fighthumantraffickingintrinidadandtobago&hl=en (дата обращения: 08.05.2020).

3 См.: World Vision, "*New Hotline Number and Smartphone App Make Reporting Trafficking Possible for more Albanians*" [website] (World Vision, 15 June 2014) [World Vision, «Новый номер горячей линии и приложение для смартфона позволяют большему количеству албанцев сообщать о торговле людьми» [веб-сайт] (World Vision, 15 июня 2014 г.)]. URL: www.worldvision.org/about-us/media-center/new-hotline-number-and-smartphone-app-makereporting-trafficking-possiblemore (дата обращения: 08.05.2020).

4 См.: Unseen, "*Unseen launches app to report modern slavery*" [website] (Unseen, 30 July 2018) [Unseen, «Unseen» запускает приложение для сообщения о современном рабстве» [веб-сайт] (Unseen, 30 июля 2018 г.)]. URL: www.unseenuk.org/news/55 (дата обращения: 08.05.2020).

включают «Missing: Game for a Cause»[1], «Act!»[2], «BAN Human Trafficking!»[3] или «Slavery Footprint»[4]. Эти игры содержат ролевые сценарии, основанные на реальных историях, и повышают осведомленность о различных формах торговли людьми.

Наиболее удобным способом/инструментом улучшения предоставления информации людям с целью предотвращения торговли людьми является использование *искусственного интеллекта* (*ИИ*).

Инструменты, применяющие ИИ, способны мгновенно отвечать на информационные запросы в любое время суток и одновременно обрабатывать большое количество запросов. Хорошим примером является приложение «MissMigration»[5], которое представляет собой чат-бот «Facebook», распространяющий ценную информацию о миграции. Чат-бот обеспечивает автоматические ответы на обычные вопросы о миграции, такие как требования к оформлению паспорта, визы и разрешения на работу, а также правила и нормативные положения, т.е. предоставляет информацию, которая может быть очень полезной для предотвращения торговли людьми.

Очевидно, что применение данных технологических инструментов, осуществляемое в рамках взаимодействия государственных структур и частного сектора, координируется и обо всех результатах выявления фактов торговли людьми должны быть извещены компетентные органы для анализа ситуации и принятия мер противодействия.

Устранение возможностей для эксплуатации: использование технологий для предотвращения, пресечения и исключения соучастия торговцев людьми в деятельности компаний. Торговцы людьми также активно используют онлайн-видеоигры

---

1 См.: «Missing Girls», «*Missing. Game for Cause*» [веб-сайт] («Missing Link Trust»). URL: www.missingirls.itch.io/missing-game-for-a-cause (дата обращения: 08.05.2020).

2 См.: Lifeboat Project, "*Learn to identify the signs*" [website] (Lifeboat Project, 2016) [Проект «Спасательная шлюпка», «Учитесь определять признаки» [веб-сайт] (Проект «Спасательная шлюпка», 2016 г.)]. URL: www.lifeboat-act.com/#about (дата обращения: 08.05.2020).

3 См.: «Balkan Act Now!» «*Ban Human Trafficking*» [веб-сайт] (Balkan Act Now! 2014 г.)]. URL: www.banhumantrafficking.com/en/ (дата обращения: 08.05.2020).

4 См.: Slavery Footprint, «*Slavery Footprint*» [веб-сайт] (Made in a Free World). URL: www.slaveryfootprint.org/#where_do_you_live (дата обращения: 08.05.2020).

5 См.: MOM, «*Miss Migration*» [веб-сайт] (MOM). URL: www.facebook.com/MissMigration (дата обращения: 08.05.2020).

для *развращения детей и сексуальной эксплуатации* их различными способами, особенно в сфере сексуальных услуг. В качестве контрмеры были разработаны технологические решения, направленные на *предотвращение попыток онлайн-развращения*, особенно детей и несовершеннолетних. Одним из примеров является технология «Project Artemis», разработанная корпорацией «Microsoft» и представляющая собой инструмент выявления методов развращения. Она позволяет обнаруживать онлайн-злоумышленников, устранять их сайты и сообщать о попытках заманить детей в целях их сексуальной эксплуатации[1].

Важным представляется то, что данная технология применяется к *ретроспективным* текстовым беседам в чате. «Project Artemis» оценивает и «ранжирует» характеристики беседы и присваивает общий рейтинг вероятности. Затем этот рейтинг можно использовать как определитель, который устанавливается каждой компанией, применяющей эту методику для принятия решения, следует ли помеченный и вызывающий подозрения диалог отправлять специалистам-модераторам для проверки. «Microsoft» объявила, что этот инструмент будет доступен другим организациям.

С учетом беспрецедентных онлайн-рисков для несовершеннолетних в сети в Китае на законодательном уровне пересмотрены и приняты упреждающие меры противодействия киберугрозам.

С 1 июня 2021 г. в Китае вступили в силу специально переработанные законы о защите несовершеннолетних и о предупреждении правонарушений среди несовершеннолетних, которые нацелены на обеспечение безопасности и более надежную защиту детей в школе и дома в режиме как онлайн, так и офлайн. Указанные законы предусматривают создание системы профилактики и борьбы с буллингом среди учащихся, который все чаще совершается в сети, механизм скрининга психического здоровья несовершеннолетних и раннего вмешательства, а также системы профилактики сексуального насилия и домогательств в отношении несовершеннолетних[2].

---

[1] См.: Courtney Gregoire, "*Microsoft shares new technique to address online grooming of children for sexual purposes*" [website] (Microsoft, 9 January 2020) [Кортни Грегуар, «Microsoft» делится новой методикой решения проблемы развращения детей онлайн в сексуальных целях» [веб-сайт] (Microsoft, 9 января 2020 г.)]. URL: www.blogs.microsoft.com/on-the-issues/2020/01/09/artemis-online-grooming-detection/ (дата обращения: 08.05.2020).

[2] 1 июня в Китае вступят в силу пересмотренные законы о защите несовершеннолетних и о предупреждении правонарушений среди несовершеннолетних // СИНЬХУА Новости. URL: http://russian.news.cn/2021–05/30/c_139978880.htm (дата обращения: 02.06.2021).

В соответствии с *Законом КНР о защите несовершеннолетних* 1991 г., доработанном в 2020 г., школы и детские сады обязаны сообщать о случаях, связанных с серьезным буллингом, фактах сексуального насилия или домогательства в отношении детей в полицию и органы по делам образования, а также своевременно принимать меры по защите жертв сексуального насилия и домогательств.

В ходе найма персонала работодатели в отраслях, имеющих тесные контакты с несовершеннолетними, должны проверять досье заявителей в полиции и прокуратуре, чтобы отсеять тех, кто имеет судимость за такие преступления, как сексуальное посягательство, жестокое обращение, торговля людьми и нанесение телесных повреждений.

Поставщикам онлайн-продуктов и сетевых услуг запрещено предоставлять несовершеннолетним продукты и услуги, способные вызывать у них зависимость. Должны быть установлены соответствующие функции управления временем, разрешениями и потреблением для несовершеннолетних, пользующихся такими онлайновыми услугами и продуктами, как игры, стриминг, социальные сети, а также размещенный в интернете аудио- и видеоконтент.

В соответствии с *Законом КНР о предупреждении правонарушений среди несовершеннолетних* 1999 г., пересмотренном в декабре 2020 г., несовершеннолетние, признанные виновными в совершении преступлений, но освобожденные от уголовного наказания в связи с тем, что они не достигли возраста уголовной ответственности, могут получить специальное коррекционное образование после оценки соответствующим экспертным комитетом. Кроме того, образовательные учреждения должны нанимать психологов по контрактам на полный или неполный рабочий день, а также активизировать контакты и сотрудничество с родителями или опекунами для совместного улучшения просветительской работы в области психического здоровья несовершеннолетних[1].

В сфере *торговли людьми в целях принудительного труда* использование технологий для расширения обмена информацией о рекрутерах и брокерах может помочь мигрантам самостоятельно выбирать более безопасные каналы миграции, тем самым сокращая возможности субъектов, замеченных в применении трудовой эксплуатации. Технологии также дают возможность для более прямого найма в обход местных брокеров (рекрутеров), которые часто зани-

[1] 1 июня в Китае вступят в силу пересмотренные законы о защите несовершеннолетних и о предупреждении правонарушений среди несовершеннолетних // СИНЬХУА Новости. URL: http://russian.news.cn/2021–05/30/c_139978880.htm (дата обращения: 02.06.2021).

мают влиятельные позиции, обладая информацией и связями. Выплаты этим брокерам могут поставить мигрантов в ситуацию долга под высокие проценты, по существу привязывая их к месту работы, что делает их чрезвычайно уязвимыми для злоупотреблений и эксплуатации.

Зарубежный опыт показывает, что онлайн-наем дает возможность обойти местных брокеров, позволив мигрантам подавать заявки на вакансию напрямую или, в случае ограниченности знаний и технологий, с помощью авторитетных институтов гражданского общества на местах или правительственной организации.

Онлайн-процесс также предусматривает *создание цифровой записи с момента подачи заявки*. В сочетании с блокчейн-технологиями появляются потенциальные средства решения проблем, связанных с наймом работников, в частности проблем подмены контрактов. Рекрутеры обманывают многих работников-мигрантов, обещая заработную плату и условия труда, которые не соответствуют действительности. В таких случаях работники подписывают контракт на благоприятных условиях с рекрутерами в стране своего происхождения, но, когда они прибывают в страну назначения, рекрутеры подменяют его на другой, гораздо менее выгодный контракт.

По оценкам исследования МОТ, подмена контракта затрагивает 43% мигрантов из Мьянмы в Таиланд, при этом письменный контракт считается менее надежным, чем устное соглашение[1].

Введение контракта каждого работника в блокчейн создает неизменяемую запись исходного контракта, оформленного работнику. Это можно использовать для проверки того, что: 1) договор соответствует применимым правовым нормам и составлен на языке, понятном мигранту, и 2) это тот же договор, который предоставляется работнику на рабочем месте.

Одним из внушающих оптимизм примеров в этом отношении является партнерство между неправительственной организацией «Mekong Club» из Гонконга, которая сотрудничает с бизнесом в целях улучшения ситуации в их цепочках поставок, и компанией «Diginex», которая использует блокчейн в коммерческих целях и тестирует применимость технологии для борьбы с некоторыми видами эксплуатации в сфере найма рабочей силы.

---

[1] См.: Benjamin Harkins, Daniel Lindgren and Tarinee Suravoranon, *Risks and rewards*: *Outcomes of labour migration in South-East Asia* (Bangkok: ILO and IOM, 2017) [Бенджамин Харкинс, Даниэль Линдгрен и Тарини Сураворанон, Риски и вознаграждение: результаты трудовой миграции в Юго-Восточной Азии (Бангкок: МОТ и МОМ, 2017 г.)]. С. 32.

Используя подход, предполагающий участие многих субъектов, «Diginex» и «Mekong Club» вместе со своими корпоративными партнерами проверяют, можно ли использовать блокчейн-технологию с ее способностью хранить неизменяемые записи для уменьшения количества случаев подмены контрактов, в том числе путем предоставления работникам с разным уровнем владения технологиями возможности загружать свою документацию лично[1].

Еще одним пилотным проектом, тестирующим применение блокчейн-технологии, является сотрудничество компании «Coca-Cola» с некоммерческой организацией «Blockchain Trust Accelerator»[2]. Это партнерство с участием многих субъектов, одним из которых является Государственный департамент США, использует защищенный реестр, обеспечиваемый данной технологией, для подтверждения контрактов с работниками. Посредством неопровержимых доказательств и обеспечения защищенности в контрактах «Coca-Cola» проверяет и анализирует, как агенты по трудоустройству взаимодействуют с работниками.

Вместе с тем существуют проблемы с использованием блокчейн-технологии, в первую очередь в связи с тем, что система надежна лишь настолько, насколько надежны вводимые данные. В примере с технологией «Diginex» риски, связанные с загрузкой контрактов рекрутерами, устраняются путем проверки контракта, размещенного в системе работником и сопровождаемого его фотографией.

Другие проблемы, связанные с использованием блокчейн-технологии для полной автоматизации процессов найма, включают доступ мигрантов к технологиям, возможность их использования и доверие к ним. Институт Иссара (Issara Institute) назвал быстрое увеличение охвата смартфонами и рост уровня грамотности ключевым компонентом усилий по сокращению практики эксплуатации труда мигрантов.

---

[1] См.: Diginex and Mekong Club, "*Combating Modern Slavery*" [website] (Diginex and Mekong Club, 2019) [«Diginex» и «Mekong Club», «Борьба с современным рабством» [веб-сайт] (Diginex и Mekong Club, 2019 г.)]. URL: www.eminproject.com/ (дата обращения: 08.05.2020).

[2] См.: Gertrude Chavez-Dreyfuss "*Coca-Cola, U.S. State Department to Use blockchain to combat forced labor.*" [website] (Reuters, 16 March 2018) [Гертруда Чавес-Дрейфус «Coca-Cola, Государственный департамент США будут использовать блокчейн для борьбы с принудительным трудом». [веб-сайт] (Рейтер, 16 марта 2018 г.)]. URL: www.reuters.com/article/us-blockchain-coca-cola-labor/coca-cola-us-state-dept-to-use-blockchain-to-combat-forcedlabor-idUSKCN1GS2PY (дата обращения: 08.05.2020).

Кроме того, некоторые государственные законы требуют наличия подписанного, засвидетельствованного и нотариально заверенного бумажного контракта и не признают «электронные контракты». Могут также возникнуть трудности с интеграцией блокчейн-решений в другие онлайн-системы, которые правительства используют для оформления виз или отработки запросов на трудоустройство (например, «e-Migrate» в Индии[1] или «Musaned» в Саудовской Аравии[2]).

Таким образом, зарубежный опыт показывает, что хотя блокчейн-технология обладает потенциалом для полной автоматизации и оцифровки многоуровневого оформления документов, требуемых в процессе миграции, в целях предотвращения трудовой эксплуатации еще предстоит преодолеть существующие проблемы доступности и некоторые препятствия в области миграционной политики.

Технологии для выявления потерпевших: новые возможности для жертв торговли людьми и других сторон для направления обращений. Результаты исследования ОБСЕ и ТАТ позволяют выделить следующие направления применения технологий, помогающих выявлять жертв торговли людьми. Они расширяют возможности: 1) самостоятельного обращения лиц, пострадавших от торговли людьми, или обращения третьих лиц; 2) преодоления языковых барьеров; 3) использования искусственного интеллекта; 4) использования цифровых методов расследования.

Технологии для обращения жертв торговли людьми. Технологические решения в этой сфере не обязательно должны быть сложными — «WhatsApp», «Facebook Messenger» или выделенный канал для СМС / текстовых сообщений / телефонных звонков предлагают несколько путей общения с жертвой, обратившейся за помощью. Приложения-мессенджеры предоставляют жертвам

---

[1] См.: Министерство иностранных дел Индии, «*eMigrate*» [веб-сайт] (Отдел по трудоустройству за рубежом Министерства иностранных дел Правительства Индии). URL: www.emigrate.gov.in/ext/ (дата обращения: 08.05.2020).

[2] См.: Министерство человеческих ресурсов и социального развития Королевства Саудовская Аравия, «*Национальная программа занятости «Musaned»* [веб-сайт] (Министерство человеческих ресурсов и социального развития Королевства Саудовская Аравия, 30 ноября 2016 г.). URL: www.youtube.com/watch?v=w24qzpNCx18 (дата обращения: 08.05.2020).

простой способ общения с поставщиками услуг или сетями персональной поддержки в режиме реального времени[1].

Так, при НПО «Поларис» существует Национальная горячая линия США по борьбе с торговлей людьми, которая позволяет широкой общественности анонимно сообщать о предполагаемых случаях торговли людьми через интернет, текстовые сообщения или бесплатные телефонные звонки. Обращения проверяются «Поларисом», после чего информация направляется в соответствующие правоохранительные органы[2].

Технологии для преодоления языковых барьеров. Основным препятствием для общения остается языковый барьер, поскольку многие жертвы не могут напрямую общаться с человеком, который потенциально способен им помочь, например с полицейскими, инспекторами труда, работниками НПО или социальными аудиторами. Несколько организаций разработали приложения для решения этой проблемы. Одним из примеров является приложение «Apprise»[3], разработанное «Mekong Club» в сотрудничестве с Институтом вычислительной техники и общества Университета ООН и сфокусированное на ситуациях с повышенным риском для потенциальных жертв трудовой эксплуатации. Поставщики услуг могут загрузить приложение на свои телефоны. Когда кого-то нужно опросить, можно выбрать анкету для соответствующей ситуации. Затем телефон передается респонденту, который выбирает свой язык, используя национальный флаг в качестве символа. После вступления респонденту, который слушает в наушниках, задают ряд вопросов, на которые он отвечает «да» или «нет». В конце собеседования приложение сводит в таблицу ответы на языке респондента, чтобы дать оценку уязвимости, в том числе желает ли респондент быть немедленно ограждена от обстоятельств, в которых он находится. Приложение не только помогает преодолевать язы-

[1] Лица, пережившие торговлю людьми, используют обычные страницы «Facebook» или каналы «WhatsApp» для связи со своими сообществами и взаимной поддержки в период реабилитации. Страницы поддержки создают чувство общности и солидарности, а поставщики услуг, работающие в социальных сетях, размещают ресурсы, такие как группы поддержки или информацию о психическом здоровье.

[2] См.: Polaris, "*U.S. National Human Trafficking Hotline*" [website] (Polaris) [Поларис, «Национальная горячая линия США по борьбе с торговлей людьми» [веб-сайт] (Поларис)]. URL: www.polarisproject.org/responding-to-human-trafficking/ (дата обращения: 08.05.2020).

[3] См.: Институт Университета ООН в Макао и «The Mekong Club», «Apprise» [веб-сайт] (Институт Университета ООН в Макао и «The Mekong Club»). URL: www.apprise.solutions/home (дата обращения: 08.05.2020).

ковые барьеры, но и устраняет ограничения, связанные с грамотностью, конфиденциальностью, временем и стоимостью.

Использование искусственного интеллекта. Новые технологии полезны для поиска и сортировки больших объемов информации, поиска и выявления моделей и выделения значения. ИИ является одним из примеров применения подобной технологии. ИИ — это моделирование процессов человеческого интеллекта машинами, особенно компьютерными системами. Данные процессы включают обучение (получение информации и правила использования информации), рассуждение (использование правил для получения приблизительных или определенных выводов) и самокоррекцию. Примеры использования *ИИ в борьбе с торговлей людьми* включают «Project Intercept», проект, разработанный неправительственной организацией «Seattle Against Slavery», проект «Spotlight», разработанный НПО «Thorn», и платформу «childsafe.ai».

Технологии обработки изображений, ИИ, особенно программное обеспечение для распознавания лиц, все чаще используются в попытках определить местонахождение жертв торговли людьми. Еще в 2009 г. корпорация «Microsoft» в партнерстве с Дартмутским колледжем разработала технологию «PhotoDNA», которая сейчас широко используется для борьбы с торговлей людьми и онлайн-контентом, содержащим сексуальную эксплуатацию детей. «PhotoDNA»[1] создает уникальную цифровую подпись изображения (известную как «хеш»), которая затем сравнивается с подписями (хешами) других фотографий для поиска копий того же изображения сексуальной эксплуатации детей. Если совпадение обнаружено, сообщение об этом направляется в такие организации, как Национальный центр пропавших и эксплуатируемых детей. Программа доступна бесплатно для правоохранительных органов и некоммерческих организаций.

Аналогичной технологией, которая используется в США для поиска потенциальных жертв в интернете с помощью распознавания лиц, является «idTraffickers»[2]. С ее помощью можно анализировать

---

[1] См.: Microsoft, "*Help stop the spread of child exploitation*" [website] (Microsoft) [Microsoft, «Помогите остановить распространение эксплуатации детей» [веб-сайт] (Microsoft)]. URL: www.microsoft.com/en-us/photodna (дата обращения: 08.05.2020).

[2] См.: idTraffickers, "*Software for law enforcement that identifies enslaved persons and traffickers*" [website] (Bashpole Software, Inc.) [IdTraffickers, «Программное обеспечение для правоохранительных органов, которое идентифицирует лиц, попавших в рабство, и торговцев людьми» [веб-сайт] (Bashpole Software, Inc.)]. URL: www.idtraffickers.com/ (дата обращения: 08.05.2020).

сообщения о пропавших лицах и онлайн-рекламу с применением биометрии и готовить оперативные сведения для их использования правоохранительными органами.

Технология «Traffic Jam», разработанная компанией «Marinus Analytics», помогает правоохранительным органам находить жертв торговли людьми и позволяет им ликвидировать организованные преступные сети. «Traffic Jam» — это набор аналитических инструментов, позволяющих экономить драгоценное следственное время и спасать уязвимых жертв благодаря быстрому превращению больших массивов данных в практически реализуемую оперативную информацию. Это программное обеспечение использует искусственный интеллект и машинное обучение, производя сплошной поиск в общедоступных данных по всему интернету и помогая выявлять модели торговли людьми. Отбирая данные с веб-сайтов общего доступа, таких как веб-сайты с эскорт-рекламой, «Traffic Jam» создает базу данных изображений, номеров телефонов и геолокационных данных, которые могут помочь выявить характерные признаки и получить доказательства совершенного преступления.

Аналогичным образом некоммерческая организация «Thorn» из Калифорнии разработала «Spotlight» — приложение, помогающее быстрее выявлять жертв торговли детьми в целях сексуальной эксплуатации. «Spotlight» использует огромный объем данных, доступных в интернете, особенно на эскорт-сайтах, и превращает их в актив для правоохранительных органов. Его задача состоит в том, чтобы повысить эффективность и результативность национальных расследований торговли людьми в целях сексуальной эксплуатации и увеличить число детей, которых удалось идентифицировать и перенаправить в соответствующие организации для получения помощи. Посредством «Spotlight» правоохранительные органы в настоящее время выявляют в среднем около 10 детей в день. Более того, специалисты, использующие «Spotlight» ежедневно, на 60% сокращают время расследования[1].

Независимая социологическая организация «NORC» при Чикагском университете, обрабатывая большой массив информации, превращает данные в *практически реализуемую оперативную информацию*. «NORC» разработала «Sex Trafficking Operations Portal» (STOP) [Портал операций по борьбе с торговлей людьми в целях

[1] См.: Thorn, "*Spotlight helps find kids faster*" [website] (Thorn) [Thorn, «Spotlight» помогает быстрее находить детей [веб-сайт] (Thorn)]. URL: www.thorn.org/spotlight/ (дата обращения: 08.05.2020).

сексуальной эксплуатации][1], который использует автоматизированный анализ данных в целях создания отчетов для правоохранительных органов о возможной онлайн-деятельности по торговле людьми.

В конце 2015 г. «Facebook» также присоединился к усилиям по борьбе с торговлей людьми в киберпространстве. Совместно с Генеральной прокуратурой Нью-Йорка «Facebook» разработал алгоритмы, которые анализируют язык, номера телефонов и изображения, используемые на его платформе, с целью выявления лиц, пострадавших от торговли людьми онлайн в целях сексуальной эксплуатации, уделяя особое внимание несовершеннолетним жертвам[2]. Хотя подробности этого процесса не раскрывались, бытует мнение, что в нем используются обширные системы распознания лиц «Facebook» для идентификации пропавших лиц по фотографиям, размещенным на платформе социальных сетей.

Организация «Seattle Against Slavery» [Сиэтл против рабства], представляющая собой коалицию, созданную населением и работающую с целью мобилизации общин на борьбу с торговлей людьми в целях сексуальной и трудовой эксплуатации, разработала в сотрудничестве с «Microsoft» проект «Intercept»[3] — программное обеспечение для оказания помощи жертвам и для сдерживания спроса на сексуальные услуги. При помощи чат-ботов, на которых используется язык, сформированный лицами, пережившими торговлю людьми и принудительную проституцию, программное обеспечение помогает местным защитникам интересов таких лиц связываться с потенциальными жертвами и оказывать им помощь.

Еще одним примером вовлечения общественности в краудсорсинг является приложение «TraffickCam». Данный инструмент предлагает пользователям делать снимки гостиничных номеров,

---

1 См.: Чикагский университет, «*Sex Trafficking Operations Portal* (*STOP*)» [веб-сайт] (NORC при Чикагском университете). URL: www.norc.org/Research/Projects/Pages/sex-trafficking-operations-portal-stop.aspx (дата обращения: 08.05.2020).

2 См.: Jeff John Roberts, "*How Facebook Will Fight Sex Trafficking*" [website] (Fortune, 8 October 2015) [Джефф Джон Робертс, «Как «Facebook» будет бороться с торговлей людьми» [веб-сайт] (Fortune, 8 октября 2015 г.)]. URL: www.fortune.com/2015/10/08/facebook-sex-trafficking/ (дата обращения: 08.05.2020).

3 См.: Seattle Against Slavery, "*Freedom Signal. Technology to Combat Online Sex Trafficking*" [website] (Seattle Against Slavery) [Seattle Against Slavery, «Сигнал свободы. Технологии борьбы с онлайн-секс-торговлей» [веб-сайт] (Seattle Against Slavery)]. URL: www.seattleagainstslavery.org/technology/ (дата обращения: 08.05.2020).

в которых они останавливаются, в то время как правоохранительные органы загружают фотографии из рекламы сексуальных услуг. Эти изображения анализируются на предмет сходства с помощью компьютерного алгоритма в национальной базе данных. Цель состоит в том, чтобы использовать доступ общественности к огромному количеству гостиничных номеров для облегчения усилий правоохранительных органов по выявлению мест, где могла иметь место торговля людьми в целях сексуальной эксплуатации.

Многие технологические инструменты, описанные в этом разделе, могут использоваться правоохранительными органами для повседневного расследования дел о торговле людьми, даже если они не разрабатывались и не управляются ими. Технология «PhotoDNA», созданная «Microsoft», например, широко применяется правоохранительными органами в поиске и удалении известных изображений сексуальной онлайн-эксплуатации детей. «Spotlight» американской НПО «Thorn» используют полицейские во всех 50 штатах США и в Канаде, и этот веб-инструмент помог выявить 14 874 ребенка, ставшего жертвой торговли людьми, и идентифицировать 16 927 торговцев людьми за последние четыре года. Цель «TraffickCam» состоит в создании базы данных изображений гостиничных номеров, по которой следователь может эффективно проводить поиск других изображений, сделанных в том же месте, что и изображение, являющееся частью расследования.

Все эти примеры наглядно показывают, что установление партнерских отношений между государственными учреждениями и частным сектором / НПО в целях успешного использования технологий в борьбе с торговлей людьми является весьма полезным и что соответствующие государственно-частные партнерства могут значительно повлиять на существующую ситуацию в данной области.

Технологии для сбора общедоступной информации в целях выявления, пресечения и предупреждения торговли людьми. Международный опыт показывает: в то время как торговцы людьми злоупотребляют социальными сетями и другими онлайн-форумами для вербовки и эксплуатации своих жертв, разведка на основе открытых источников и расследования с использованием социальных сетей также являются полезными инструментами в борьбе с торговлей людьми.

Разведка на основе открытых источников — это использование информации, полученной из источников общего доступа, в оперативно-разведывательном контексте. Размер и объем данных из открытых источников неизмеримо увеличивались по мере развития

технологий и распространения общедоступной информации в интернете. Эти данные могут содержать обширную информацию, важную для выявления преступлений и проведения расследований в отношении как торговцев людьми, так и их жертв.

В качестве успешного примера использования данных из открытых источников для создания препятствий торговцам людьми в их преступной деятельности можно привести базу данных «World Check». С 2015 г. «Thomson Reuters» в сотрудничестве с неправительственной организацией «Liberty Asia» успешно использовала информацию из открытых источников для выявления и внесения в черный список более чем 5 тыс. осужденных торговцев людьми. Отслеживая мировые онлайн-СМИ, эти организации подтверждают личности преступников, осужденных за торговлю людьми, и их данные затем загружаются в базу данных «World Check», составленную «Thomson Reuters». «World Check» не является инструментом, разработанным специально для случаев торговли людьми, и представляет собой платформу общего характера для проверки личности. Однако эта база данных позволяет международному бизнес-сообществу безопасно и точно передавать информацию о лицах и организациях, осужденных за торговлю людьми, предоставляя ему возможность принимать информированные решения о том, с кем вести дела, и затрудняя торговцам людьми задачу сокрытия, отмывания и перемещения своих незаконных доходов по всему миру[1]. Это хороший пример того, как универсальная технология может быть использована в борьбе с торговлей людьми.

Результаты исследования зарубежного и отечественного опыта показывают, что распространенным методом привлечения жертв является применение торговцами людьми фальшивых профилей в социальных сетях для размещения ложных или вводящих в заблуждение объявлений о вакансиях. Однако большинство приложений для общения в социальных сетях, чатов и подобных пространств могут предоставить оперативным сотрудникам, ведущим дела по торговле людьми, такую же анонимность, что и преступникам. Это позволяет оперативным сотрудникам безопасно и уда-

[1] См.: Thomson Reuters, "*Thomson Reuters World-Check and Liberty Asia exceed 5,000 names in anti-human trafficking initiative*" [website] (Thomson Reuters, 18 June 2017) [Thomson Reuters, «World-Check» «Thomson Reuters» и «Liberty Asia» внесли в списки свыше 5000 имен в рамках инициативы по борьбе с торговлей людьми» [веб-сайт] (Thomson Reuters, 18 июня 2017 г.)]. URL: www.thomsonreuters.com/en/press-releases/2017/june/thomson-reutersworld-check-and-liberty-asia-clear-5000- names-in-anti-human-trafficking-initiative.html (дата обращения: 08.05.2020)

ленно общаться с потерпевшими и правонарушителями под видом потенциальных клиентов или потенциальных жертв для сбора доказательств виновности торговцев людьми. Из учетных записей социальных сетей можно получить большой объем полезных данных о правонарушителях, в том числе об их образе жизни, соучастниках и активах — это те подробности, которые можно использовать для успешного расследования и судебного преследования.

Эффективным способом выявления латентных форм торговли людьми являются *расследования под прикрытием*, в ходе которых сотрудники оперативных подразделений используют вымышленные онлайн-личности для выявления преступников или жертв и взаимодействия с ними. Данный способ широко применяется правоохранительными органами по всему миру. Проведение подобных расследований с использованием социальных сетей и других онлайн-платформ, таких как сайты тематической рекламы, дает ряд преимуществ. Сотрудники под прикрытием могут собирать сопоставимый объем информации, используя меньше ресурсов и не попадая в потенциально опасные ситуации, возможные при личной встрече с правонарушителями.

Использование социальных сетей и других интернет-платформ для онлайн-расследований стало обычным и популярным методом оперативных сотрудников, работающих с делами по торговле людьми в некоторых государствах — участниках ОБСЕ.

Примерами технологических инструментов в этой области являются «Project Intercept», реализуемый американской НПО «Seattle Against Slavery», и «childsafe.ai»[1], которые могут быть использованы для создания фальшивой онлайн-личности с целью установления прямого контакта с торговцами людьми, жертвами или покупателями.

Большинство ведущих социальных сетей и других онлайн-платформ готовы сотрудничать с правоохранительными органами и передавать запрашиваемые данные о потенциальных правонарушителях после предъявления соответствующих юридических предписаний.

Технологии в оценке рисков: выявление риска торговли людьми для повышения бдительности, например, в цепочках поставок частного сектора. Еще одной областью, в которой технология позволяет просматривать большие объемы информации,

[1] См.: childsafe.ai, "*The Artificial Intelligence Platform Protecting Kids Online*" [website] (childsafe.ai, Inc) [childsafe.ai, «Платформа искусственного интеллекта, защищающая детей в Интернете» [веб-сайт] (childsafe.ai, Inc)]. URL: www.childsafe.ai (дата обращения: 08.05.2020).

является *оценка рисков*. Многонациональная компания может иметь тысячи поставщиков по всему миру со своими кодексами поведения и трудовыми стандартами, применение которых ожидается и от каждого из их поставщиков. Такие компании проводят аудиты на местах, чтобы убедиться, что поставщик соблюдает соответствующие стандарты. Подобные фирмы все чаще осознают свою ответственность за недопущение торговли людьми в своей деятельности отчасти из-за законов о раскрытии информации, недавно принятых в Великобритании, Франции, США и Австралии.

«Target Corporation» на корпоративном уровне наладила партнерство с организацией «Goodweave International»[1], которая занимается искоренением *детского труда* с упором на ковровую промышленность в Южной Азии. «Target Corporation» пилотирует базу данных, в которой аккумулируются и обобщаются данные инспекций и аудитов субъектов в цепочке поставок компании в Индии.

Применяемая технология также предусматривает возможность проведения анонимных опросов и получения отзывов работников[2]. Затем обобщенные данные отображаются на информационной панели, которая позволяет менеджерам цепочки поставок «Target» принимать решения относительно соблюдения прав человека субъектами в цепочке поставок. Пользователи могут анализировать демографические тенденции и предпринимать целенаправленные действия.

«The Mekong Club» также собирает данные аудитов, чтобы помочь компаниям определить зоны риска. Его «матрица оценки рисков» включает более 15 тыс. строк аудиторских данных из 25 стран, собранных в формате, позволяющем сравнивать различные параметры из разных стандартов аудита и наборы вопросов. Данные классифицируются в соответствии с ключевыми показателями принудительного труда на основе критериев МОТ, а также дополнительных показателей (например, связанных с наймом мигрантов) страны и региона. Далее они подразделяются на категории по виду продукции (обувь, одежда, аксессуары и пр.) и процессу

---

[1] См.: Target, "*Crafting a Better Tomorrow*: *Target Joins Forces with GoodWeave*" [website] (Target, 2 September 2015) [Target, «Создавая лучшее будущее: «Target» объединяет усилия с «GoodWeave» [веб-сайт] (Target, 2 сентября 2015 г.)]. URL: www.corporate.target.com/article/2015/09/goodweave-partnership (дата обращения: 08.05.2020).

[2] См.: USAID, «*Инициатива «Supply Unchained»* [веб-сайт] (USAID). URL: www.partnerships.usaid.gov/partnership/supply-unchained-initiative (дата обращения: 08.05.2020).

(производственный процесс, относящийся к 1-му уровню, обработка и компоненты, относящиеся ко 2-му уровню, или сырье, относящееся к 3-му уровню).

Пользователи могут получить доступ к следующей информации: 1) виды нарушений трудовых прав, выявленных в ходе проверок; 2) информация об общем количестве проведенных аудитов и количестве обнаруженных проблем. Это дополняется данными на уровне страны и информацией «Apprise Audit».

Анализ такого огромного количества информации для выявления случаев торговли людьми был бы невозможен без использования технологий.

Вместе с тем международные эксперты ОБСЕ и ТАТ предупреждают, что результаты аудитов могут быть сфальсифицированы или подвержены влиянию других факторов. Такие ошибочные данные могут отрицательно сказаться на достоверности анализа, создавая неполную или неточную картину того, действует ли поставщик этично и соблюдаются ли права работников.

Технологии могут помочь решить эту проблему за счет 1) улучшения вклада сотрудников в процессы аудита и мониторинга, 2) дополнения данных аудита путем обеспечения доступа к другим источникам информации и их обработки. Это могут быть новостные отчеты, судебные документы, публичные записи или любые материалы, которые ставят под сомнение данные из открытых источников о поставщике и его деловых партнерах[1]. Низкотехнологичный вариант этого метода — поиск по словам, при котором компании могут сканировать интернет по ключевым словам, связанным с принудительным трудом и торговлей людьми.

Данная информация также может выступать в качестве профилактической меры. Американская компания — разработчик программного обеспечения «SAP Ariba» сотрудничает с организацией «Made in a Free World», которая использует ИИ, аналитическое программное обеспечение и облачные технологии для анализа цепочек поставок. Благодаря обобщению данных из открытых источников и других данных это программное обеспечение позволяет менеджеру цепочки поставок получать доступ к открытым данным

[1] См.: Samir Goswami, "*Testimony to the Tom Lantos Human Rights Commission in the U.S. Congress*", *Hearings on Artificial Intelligence*: *The Consequences for Human Rights* (July 2018) [Самир Госвами, «Свидетельство комиссии по правам человека Тома Лантоса в Конгрессе США», Слушания по искусственному интеллекту: последствия для прав человека (июль 2018 г.)]. URL: www.humanrightscommission.house.gov/events/hearings/artificialintelligence-consequences-human-rights (дата обращения: 08.05.2020).

о поставщиках, оценивая их на предмет создания ими рисков для соблюдения трудовых прав.

Технологии и упреждающий мониторинг ситуаций, в которых существует риск подвергнуться эксплуатации. Понимание того, что применяемые механизмы, такие как аудит, имеют ограничения для выявления случаев торговли людьми и принудительного труда в цепочках поставок компаний, вынудило искать новые методы выявления фактов противоправных деяний как на рабочем месте, так и в процессе найма работников.

В частности, компании и группы социальной защиты работников активизировали усилия по общению с ними в форме обратной связи и инициатив типа «голос работника». На рынке представлен ряд продуктов, в которых используются мобильные и другие технологии для опроса работников или определения масштабов торговли людьми. Эти продукты могут дополнять очные, традиционные методы сбора данных и позволяют связываться с людьми посредством знакомых им технологий. Кроме того, низкие затраты и возможность оперативно проводить оценку вероятности эксплуатации работников позволяют предпринимать действия для быстрого установления связи с целевыми группами и реагировать на проблемы по мере их появления в режиме реального времени.

Одним из примеров является платформа «GeoPoll»[1], которая позволяет проводить опросы через СМС, интерактивный автоответчик (IVR) и мобильное приложение для связи с фермерами, шахтерами, фабричными рабочими, рыбацкими общинами и другими лицами, которые были свидетелями или сталкивались с нарушениями трудовых отношений. Опросы можно проводить одноразово или периодически в течение определенного периода для мониторинга условий и оценки принятых мер. Сеть компании насчитывает 225 млн пользователей в более чем 40 странах Африки, Азии и Ближнего Востока, и она может настраивать проведение опросов по местоположению (регион, город, округ, деревня) и демографическим характеристикам (пол, возраст). Платформа «GeoPoll» отправляет опросы через СМС или интерактивный автоответчик (IVR), бесплатные для респондентов. Информация собирается анонимно. Опросы обычно включают от 15 до 25 вопросов, при этом некоторые из них касаются распространенности торговли людьми, детского и принудительного труда.

[1] См.: GeoPoll, "*GeoPoll Solutions*" [website] (GeoPoll) [GeoPoll, «Решения «GeoPoll» [веб-сайт] (GeoPoll)]. URL: www.geopoll.com/geopollsolutions/ (дата обращения: 08.05.2020).

«Labourlink»[1] — другой инструмент для получения обратной связи от работников с целью выявления случаев торговли людьми. Это мобильная платформа, которая устанавливает двусторонний канал связи, позволяющий сотрудникам обмениваться мнениями в режиме реального времени, а организациям — иметь четкую картину положения сотрудников в их цепочках поставок. С 2010 г. технология «Laborlink» была развернута более чем в 20 странах и охватила более 3 млн сотрудников по всему миру. Темы опросов касаются принудительного труда и этичного обращения, здоровья и безопасности, механизмов подачи жалоб, сексуальных домогательств и здоровья женщин.

Еще один технологический инструмент — «Ulula» — объединяет платформу для рассмотрения жалоб с опросами об условиях труда, используя автоматизированные опросы, бесплатные СМС, голосовые вызовы и мессенджер «Facebook» для привлечения заинтересованных сторон и оценки экологических, социальных и управленческих рисков. Он может классифицировать и отображать информацию в соответствии с ключевыми экологическими, социальными и управленческими индикаторами в режиме реального времени, обеспечивая быструю обратную связь[2]. Примерами программ установления связи с работниками являются также пилотный проект ICTI «Ethical Toys Program Worker Voice Pilot»[3] и горячая линия «Adidas Fair Play» — внутренний механизм рассмотрения жалоб для всех сотрудников по всему миру.

Все большую роль в выявлении жертв торговли людьми и преступников играет анализ финансовых операций и финансового сектора. В большинстве государств — участников ОБСЕ банки и другие финансовые учреждения уполномочены отслеживать подозрительные операции и сообщать о них подразделениям финансовых расследований. От банков и финансовых учреждений обычно

---

1 См.: Elevate, "*Worker Engagement*" [website] (Elevate Limited) [Elevate, «Вовлечение работников» [веб-сайт] (Elevate Limited)]. URL: www.elevatelimited.com/services/consulting/worker-engagement/ (дата обращения: 08.05.2020).

2 См.: Ulula, "*Stakeholder Engagement for Responsible Supply Chains*" [website] (Ulula LLC) [Ulula, «Взаимодействие с заинтересованными сторонами для создания ответственных цепочек поставок» [веб-сайт] (Ulula LLC)]. URL: www.ulula.com/product/ (дата обращения: 08.05.2020).

3 См.: ICTI Ethical Toy Program, "*Worker Helpline*" [website] (International Council of Toy Industry) [ICTI, Программа этических игрушек, «Телефон доверия для работников» [веб-сайт] (Международный совет индустрии игрушек)]. URL: www.ethicaltoyprogram.org/en/our-program/worker-engagement/worker-helpline/ (дата обращения: 08.05.2020).

требуется, чтобы они передавали информацию о вызывающих подозрение операциях, связанных с отмыванием денег или террористической деятельностью. Тем не менее есть хорошие примеры, когда власти, банки и финансовые учреждения проявляют инициативу и сосредоточиваются конкретно на выявлении возможных случаев торговли людьми.

Активное участие банков и других финансовых учреждений в борьбе с торговлей людьми имеет важное значение из-за их способности обнаруживать финансовые потоки незаконных средств, перемещаемых организованными группами, и наличия возможности выявлять случаи торговли людьми без необходимости дожидаться обращения жертв с жалобой об эксплуатации. Связь между финансовым сектором, технологиями и торговлей людьми можно объяснить тем, что анализ финансовых операций с целью выявления случаев торговли людьми осуществляется посредством специального программного обеспечения, разработанного банками на основе алгоритмов, учитывающих индикаторы торговли людьми. Более современное программное обеспечение с высокой производительностью обработки, адаптированное к таким характерным признакам, лучше подходит для выявления подобных случаев.

Проект «PROTECT»[1] в Канаде является недавним примером того, как использование индикаторов торговли людьми для анализа финансовых операций может привести к обнаружению этого преступления и идентификации его исполнителей. Данный проект представляет собой государственно-частное партнерство между Центром анализа финансовых транзакций и отчетности Канады (FinTRAC), финансовыми учреждениями и правоохранительными органами, которые используют движение денежных средств для выявления и расследования преступлений, совершаемых торговцами людьми. Подразделения банков по борьбе с отмыванием денег начинают помечать красными флажками подозрительные счета, основываясь на таких показателях, как многократное бронирование мотелей, большие расходы в аптеках и частые депозиты в банкоматах посреди ночи. Они сообщают о подозрительной активности в FinTRAC, который, в свою очередь, уведомляет правоохранительные органы.

[1] См.: Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), “Project PROTECT. Public Service Renewal in Action” [website] (FINTRAC, 16 August 2019) [Канадский центр анализа финансовых операций и отчетности (FINTRAC), «Project «PROTECT». Обновление государственной службы в действии» [веб-сайт] (FINTRAC, 16 августа 2019 г.)]. URL: www.fintrac-canafe.gc.ca/emplo/psr-eng (дата обращения: 08.05.2020).

Другим аналогичным примером является Банковский альянс США против торговли людьми (USBA), в который входят «American Express», «Bank of America», «PayPal», «Deutsche Bank», а также Министерство внутренней безопасности США, окружной прокурор округа Нью-Йорк и НПО «Поларис». Инструменты, созданные Альянсом, используются банками-участниками в их внутренних системах для поиска индикаторов и определения динамики в больших наборах финансовых данных, которые могут указывать на причастность к торговле людьми. Представители гражданского общества, обладающие экспертными знаниями в этой области, консультируют сотрудников финансового сектора относительно того, что именно им следует искать. В частности, это могут быть: 1) перевод денежных средств обратно работодателю или тому же третьему лицу после выплаты заработной платы (возможное погашение долга); 2) относительно высокие расходы на статьи, не соответствующие заявленной цели, такие как аренда нескольких квартир (жилье для работников); 3) бизнес-клиенты, совершающие регулярные операции в нерабочее время (например, совершение оплаты в 2 часа ночи в маникюрном салоне, что может указывать на возможную проституцию). Банки-участники также собирают данные, которые могут использоваться в качестве доказательств в делах против торговцев людьми.

Как заявил окружной прокурор округа Нью-Йорк Сайрус Вэнс-младший Фонду «Thomson Reuters», «*такой сбор достоверных данных показывает движение денег и кому принадлежат кредитные карты. Подобные вещи являются косвенными и прямыми доказательствами, неопровержимыми доказательствами, позволяющими выстраивать эти дела*»[1].

Кроме того, фонд «Thomson Reuters Foundation» сотрудничал с Европейским банковским альянсом, в который входят «Barclays», «HSBC», «Standard Charter» и «UBS», для разработки инструментария, обучающего банковский персонал обнаружению признаков торговли людьми среди лиц, оформляющих вклады в отделениях, а также для проведения прецедентных исследований и разработки инструментов, позволяющих аналитикам выявлять «подозри-

[1] См.: Ellen Wulfhorst, "*Banks get tools to spot human traffickers moving illicit profits*" [website] (Reuters, 19 July 2018) [Эллен Вулфхорст, «Банки получают инструменты для выявления торговцев людьми, перемещающих незаконную прибыль» [веб-сайт] (Рейтер, 19 июля 2018 г.)]. URL: www.reuters.com/article/usa-trafficking-banking/rpt-banks-get-tools-to-spot-human-traffickers-moving-illicit-profits-idUSL8N1UF4LU (дата обращения: 08.05.2020).

тельные модели финансовой деятельности» и сообщать о них[1]. Аналогичная работа с банками проводится в Азии, где Фонд «Thomson Reuters» и «The Mekong Club» поддерживают «Азиатско-Тихоокеанский банковский альянс против торговли людьми», который недавно выпустил «Белую книгу»[2] как продолжение того, что уже было сделано в ЕС и США.

Подход, предполагающий участие многих субъектов, часто используется при разработке и внедрении технологий в борьбе с торговлей людьми. Независимо от того, используются ли они для вовлечения работников или выявления возможных случаев торговли людьми, большинство технологий и технологических инструментов являются результатом партнерства между различными организациями. Кроме того, некоторые из упомянутых в этом разделе инструментов могут помочь правоохранительным органам в идентификации жертв и преступников и в расследовании дел.

Так, проект «PROTECT» в Канаде, ориентированный на банковский сектор, значительно увеличил количество сообщений о предполагаемых случаях торговли людьми, направленных правоохранительным органам по результатам анализа финансовых операций.

Технологии в выявлении типологий в механизме торговли людьми и соответствующие действия — поиск в больших массивах данных и системный анализ. Технологии играют важную роль в сборе, обобщении и анализе данных, что позволяет выявлять тенденции и схемы торговли людьми. Это очень важно для разработки стратегических ответных мер, направленных на противодействие этим преступлениям, и для обеспечения эффективного распределения человеческих и финансовых ресурсов.

---

[1] См.: Thomson Reuters Foundation, *Thomson Reuters Foundation launches toolkit to tackle human trafficking with financial data* (Thomson Reuters Foundation, 2 May 2017) [Thomson Reuters Foundation, Фонд «Thomson Reuters Foundation» запускает набор инструментов для борьбы с торговлей людьми, используя финансовые данные (Thomson Reuters Foundation, 2 мая 2017 г.)]. URL: www.trust.org/contentAsset/raw-data/4a50dde4-0a6c-49f9-9ba4-92a8b10d3243/document (дата обращения: 08.05.2020).

[2] См.: Thomson Reuters Foundation, "*Thomson Reuters Foundation and The Mekong Club launch resource for financial institutions in Asia Pacific to combat modern slavery*" [website] (Thomson Reuters Foundation, 2019) [Thomson Reuters Foundation, «Thomson Reuters Foundation» и «The Mekong Club» запускают ресурс для финансовых учреждений в Азиатско-Тихоокеанском регионе по борьбе с современным рабством» [веб-сайт] (Thomson Reuters Foundation, 2019 г.)].

Интернет безграничен, а торговля людьми может совершаться на тысячах онлайн-платформ. В отсутствие инструментов обобщения и анализа данных ручной просмотр и анализ подобных платформ правоохранительными органами, НПО или политиками нереален, особенно с учетом того, что последний необходимо обновлять и перепроверять с определенной периодичностью.

Хорошим примером использования технологий для анализа глобальных и региональных преступных схем является «Counter-Trafficking Data Collaborative» (CTDC) [Совместный центр данных по борьбе с торговлей людьми], первый такого рода глобальный центр, публикующий гармонизированные данные, полученные от организаций по борьбе с торговлей людьми по всему миру.

Данные о торговле людьми часто содержат информацию настолько чувствительного свойства, что ее размещение может вызвать опасения, связанные с конфиденциальностью и гражданскими свободами: риск идентификации субъектов персональных данных может быть высоким, а последствия — серьезными. «CTDC» использует современные технологии для преодоления этих проблем и обеспечивает беспрецедентный публичный доступ к крупнейшим в мире массивам данных о торговле людьми. Объединение глобальных данных на одной платформе укрепляет местные, национальные и международные институты и дает им возможность успешнее бороться с торговлей людьми и эксплуатацией[1].

«Tellfinder» (ранее «Memex») — это еще одна продвинутая технология с различными функциями, включая обобщение данных для выявления ключевых лиц и организаций, причастных к торговле людьми, и обнаружение тенденций и аномальных значений с помощью ИИ для автоматического сообщения, сформированного на основе языкового контента или изображений, об индикаторах высокого риска или данных, содержащих ценную информацию[2].

Хорошо известно, что сбор данных до сих пор остается проблемой в области борьбы с торговлей людьми. Скрытый характер

---

[1] См.: Counter Trafficking Data Collaborative, "*The Counter Trafficking Data Collaborative. Global Data Hub on Human Trafficking*" [website] (IOM, Polaris and Liberty Shared, 2018) [Counter Trafficking Data Collaborative, «The Counter Trafficking Data Collaborative. Глобальный центр данных по торговле людьми» [веб-сайт] (МОМ, «Polaris» и «Liberty Shared», 2018 г.)]. URL: www.ctdatacollaborative.org/about-us (дата обращения: 08.05.2020).

[2] См.: Uncharted, "*Tellfinder. Expose Hidden Connections*" [website] (Uncharted Software Inc, 2018) [Uncharted, «Tellfinder». Раскрытие скрытых связей» [веб-сайт] (Uncharted Software Inc, 2018 г.)]. URL: www.uncharted.software/product/tellfinder/ (дата обращения: 08.05.2020).

преступления и разнообразие его типологий усложняют сбор данных, методы и методология которого отличались бы последовательностью. Проведение такой работы «в личном порядке» может быть дорогостоящим, занимать много времени и требовать принятия дополнительных мер для обработки и анализа информации. Так, команде исследователей обычно нужно время, чтобы установить необходимые отношения в этой области, завоевать доверие респондентов и участвовать в очном сборе данных посредством проведения опросов. Вот почему в настоящее время технологии все чаще используются для повышения эффективности сбора данных «в личном порядке», особенно при попытках определить масштабы торговли людьми.

Например, «IST Research»[1] — это организация, расположенная в США и использующая различные методы для оценки распространенности торговли людьми. Недавно она стала партнером Глобального фонда по искоренению современного рабства в проведении исследований, при том что первоначальные работы такого рода проводились в Южной и Юго-Восточной Азии. В настоящее время «IST» занимается исследованиями для оценки количества лиц, находящихся в условиях эксплуатации, путем комбинирования множества каналов сбора данных, включая полевой сбор данных, центры обработки вызовов, коммуникацию в социальных сетях, интерактивные автоответчики и пр. Эти различные инструменты позволяют «IST» охватить целевую аудиторию через каналы, которыми она уже пользуется. Кроме того, «IST» может отслеживать одних и тех же лиц и опрашивать их в разное время для более глубокого динамического анализа.

По оценкам «IST», традиционное исследование распространенности может занять до 18 месяцев и стоить очень дорого. Использование социальных сетей, опросов по мобильным телефонам и других каналов позволяет проводить изучение масштабов торговли людьми при значительном сокращении затрат и времени.

Методологии, основанные на технологиях, позволяют быстро увеличить эффективность методов сбора как качественных, так и количественных данных. Этот подход также может использоваться для мониторинга и оценки, чтобы измерить влияние мероприятий на местах, создавая прямую линию связи с бенефициарами

[1] См.: IST Research Corporation, «*IST Research*» [веб-сайт] (IST Research Corporation, 2018 г.). URL: www.istresearch.com (дата обращения: 08.05.2020).

для фиксирования их опыта в режиме реального времени, а также для информирования о дальнейших мероприятиях.

Этические основы и защита данных

По результатам масштабного исследования международного опыта использования онлайн-технологий в механизме торговли людьми эксперты ОБСЕ и ТАТ обращают внимание на то, что субъекты, планирующие использовать технологии для наращивания своих усилий в борьбе с торговлей людьми, должны принимать во внимание некоторые важные аспекты, связанные с конфиденциальностью данных, этикой и информированным согласием. Большинство технологических приложений для противодействия торговле людьми требуют той или иной формы сбора, хранения, обмена и анализа данных, каждая из которых имеет присущие ей риски и требует определенных мер защиты. Так, НПО может получить финансирование для разработки приложения, направленного на оказание поддержки и услуг жертвам и лицам, пережившим торговлю людьми, но не пройти обучение по вопросам безопасности, необходимое для надлежащей защиты собираемых ею данных.

Правоохранительные органы могут использовать технологическое решение, разработанное НПО или компанией частного сектора для более эффективного расследования дел о торговле людьми, но не иметь необходимых протоколов и правил для раскрытия и распространения данных, полученных с помощью этого технологического решения. Аналогичным образом компания — разработчик программного обеспечения может проявить готовность разработать и передать свою технологию субъектам борьбы с торговлей людьми, но ее коллектив может не обладать пониманием культурных традиций населения, которому она стремится помочь.

Управление рисками, связанными с конфиденциальностью данных, этикой и информированным согласием, имеет огромное значение в делах по торговле людьми, поскольку субъекты персональных данных — это жертвы эксплуатации. Травмы жертв могут усилиться, если доступ к их данным и историям получат третьи стороны, что приведет к эффекту, обратному тому, который ожидался при разработке технологий для борьбы с торговлей людьми.

Сокращение рисков, связанных с конфиденциальностью данных и этичным использованием информации в делах по торговле людьми, требует прежде всего тесного сотрудничества и постоянной коммуникации между технологическими компаниями, правоохранительными органами, лицами, пережившими торговлю

людьми, и НПО, предоставляющими поддержку и защиту жертвам торговли людьми и лицам, пережившим торговлю людьми.

Такое сотрудничество гарантирует, что НПО предоставляют необходимые рекомендации о видах информации, которые могут быть получены от жертв, и о том, как собирать информацию, не нанося дополнительных травм жертвам, а технологические компании, в свою очередь, разрабатывают необходимые технические ресурсы для сохранения собранной информации в безопасности и предотвращения несанкционированного доступа со стороны третьих лиц.

В своем отчете по этике и персональным данным Институт Иссара отмечает: «Поскольку все больше организаций, занимающихся борьбой с торговлей людьми и ответственным наймом, обрабатывают цифровую информацию и данные об обслуживаемых ими группах населения, существует острая необходимость в установлении этических стандартов и подходов. Цифровые технологии, такие как мобильные телефоны, социальные сети и программное обеспечение для анализа данных, предоставляют множество возможностей для решения проблемы торговли людьми и ответственного найма. Одновременно эти инструменты несут в себе новый комплекс негативных воздействий, рисков и угроз для уязвимых лиц»[1].

В связи с этим в рамках этических основ использования технологий в сфере борьбы с торговлей людьми предлагается семь руководящих принципов: 1) не навредить: быть сострадательными, но нейтральными; 2) приоритет личной безопасности и защиты: определить и минимизировать риски; 3) получить информированное согласие без принуждения; 4) обеспечить максимально возможную анонимность и конфиденциальность; 5) надлежащим образом подбирать и готовить переводчиков и полевые группы; 6) подготовить справочную информацию и быть готовым к экстренным действиям; 7) не стесняться помогать другим: использовать полученную информацию им на пользу.

Еще одной инициативой, авторы которой решительно выступают за этичное использование данных и информации, является

[1] См.: Rende Taylor, Lisa Maria and Mark Latonero, *Updated Guide to Ethics and Human Rights in Anti-Trafficking*: *Ethical Standards for Working with Migrant Workers and Trafficked Persons in the Digital Age* (Bangkok: Issara Institute, 2018) [Ренде Тейлор, Лиза Мария и Марк Латонеро, Актуализированное руководство по этике и правам человека в борьбе с торговлей людьми: этические стандарты работы с трудящимися-мигрантами и жертвами торговли людьми в эпоху цифровых технологий (Бангкок: Институт Иссара, 2018 г.)]. С. 46.

«Worker Engagement Supported by Technology» [Вовлечение работников при поддержке технологий] («WEST Principles»). Данная инициатива «направлена на обеспечение максимального воздействия усилий, сопровождаемых применением технологий, по выявлению и устранению риска злоупотреблений и эксплуатации работников в глобальных цепочках поставок»[1].

«WEST Principles» рекомендует организациям, планирующим использовать технологии в борьбе с торговлей людьми, оценить риски кибер- и цифровой безопасности по всей цепочке хранения данных, подготовить соответствующие планы сокращения рисков с учетом входящей информации от работников или их представителей и разработать надежные протоколы управления данными для предотвращения злоупотреблений ими. Более того, «WEST Principles» выступает за использование количественных данных для выявления возможностей улучшения условий труда в различных отраслях, стимулирования поведенческих изменений и укрепления существующего взаимодействия в целях продвижения системных реформ.

Международный опыт предполагает, что при активизации усилий по противодействию торговле людьми путем разработки и использования передовых технологий все участники этого процесса должны обеспечить наиболее полный охват аспектов, касающихся прав человека, конфиденциальности данных, этики и информированного согласия, в противном случае могут возрасти риски, связанные как раз с негативным, а не с позитивным воздействием технологий на борьбу с торговлей людьми.

Рекомендации правительствам государств — участников ОБСЕ, касающиеся правоохранительной деятельности

Заслуживают внимательного изучения и реализации рекомендации правительствам государств — участников ОБСЕ, касающиеся правоохранительной деятельности, выработанные по результатам исследования экспертами ОБСЕ и ТАТ международного/зарубежного опыта противодействия онлайн-торговле людьми.

Правительствам рекомендуется рассмотреть возможность расширения ресурсной поддержки технологических решений для государственных органов, правоохранительных структур,

[1] См.: WEST Principles, "*WEST PRINCIPLES. Worker Engagement Supported by Technology*" [website] (WEST Principles, 2017) [WEST Principles, «WEST PRINCIPLES. Вовлечение работников при поддержке технологий» [вебсайт] (WEST Principles, 2017 г.)]. URL: www.westprinciples.org (дата обращения: 08.05.2020).

занимающихся выявлением случаев торговли людьми. Это предполагает оказание поддержки: 1) инспекторам труда в использовании ими технологических приложений для проверки обращения с персоналом на предприятиях и обеспечения соблюдения национального трудового законодательства; 2) правоохранительным органам для *значительного расширения их возможностей* в борьбе с сексуальной эксплуатацией в интернете и вербовкой жертв через мошеннические предложения трудоустройства в сети.

Правительствам рекомендуется рассмотреть возможность расширения ресурсной поддержки и обучения сотрудников федеральных и региональных правоохранительных органов и поставщиков услуг для повышения эффективности использования технологических решений.

Правоохранительные органы должны еще активнее использовать возможности, которые новые технологии предоставляют для борьбы с торговлей людьми, они не должны отставать от торговцев людьми, злоупотребляющих этими технологиями.

Поставщикам услуг необходимо использовать технологические инструменты, чтобы иметь возможность предоставлять услуги жертвам торговли людьми — максимально быстро, безопасно и надежно. Поэтому правительствам следует выделять достаточные ресурсы, в том числе необходимое программное обеспечение, оборудование и обучение, чтобы правоохранительные органы и поставщики услуг имели возможность воспользоваться специализированными технологиями и инструментами, которые могли бы повысить интенсивность борьбы с торговлей людьми.

Обучение должно охватывать не только прямое использование инструментов, но и их этичное использование с учетом прав человека и защиты данных.

Правительствам рекомендуется рассмотреть вопрос о расширении ресурсной поддержки и обучении политиков, сотрудников правоохранительных органов, поставщиков услуг, НПО и представителей научных кругов, чтобы понять многочисленные способы злоупотребления технологиями со стороны торговцев людьми.

Методы торговли людьми, осуществляемой с применением технологий, имеют свои специфические особенности. Технологии позволяют торговцам людьми скрывать свою настоящую личность, повышать свою анонимность в интернете и по-новому эксплуатировать жертв. Эти современные тенденции имеют важные последствия для борьбы с торговлей людьми и могут усложнить выявление торговцев людьми и привлечение их к ответственности.

В результате все, кто участвует в борьбе с торговлей людьми, — политики, правоохранительные органы, поставщики услуг, НПО и представители научных кругов — должны пройти подготовку для лучшего понимания того, как торговцы людьми злоупотребляют технологиями. Невозможно разработать эффективные меры противодействия торговле людьми с применением технологий, если соответствующие субъекты не обладают хорошим знанием того, как торговцы людьми используют технологии в своих интересах. Наращивание потенциала в этой области может принести пользу и частному сектору, поскольку, как подтверждают результаты проведенного исследования зарубежного опыта, технологические компании играют активную роль в разработке соответствующих инструментов.

Ю.Н. Жданов, В.С. Овчинский

Международное сотрудничество в борьбе с транснациональной организованной преступностью и терроризмом: специальные методы расследования, электронные доказательства, цифровые технологии

В Справочном документе, подготовленном Секретариатом Конференции участников Конвенции ООН против транснациональной организованной преступности в мае 2020 г. (CTOC/COP/WG.3/2020/3), отмечено, что в последние годы произошли значительные изменения в методологии выявления и расследования преступлений, а также в характере следственной работы, в которой ***стали шире применяться упреждающие действия, планируемые на основе данных, полученных оперативным путем***. Кроме того, быстро совершенствуются ***технические средства негласного сбора информации***, работа с которыми часто предполагает применение ***специальных методов расследования***. Учитывая, что преступники действуют все более изощренно, соответственно и методы выявления и расследования преступлений также необходимо совершенствовать и адаптировать.

Специальные методы расследования (которые являются фактически ***аналогом оперативно-розыскных мероприятий согласно российскому законодательству***) отличаются от обычных методов и включают как скрытые действия, так и использование технических возможностей. Они особенно полезны в борьбе с профессионально организованными преступными группами (ОПГ), поскольку раскрытие преступных операций и сбор информации и доказательств, необходимых для внутригосударственного судебного преследования и уголовного производства, сопряжены с риском и трудностями.

Специальные методы расследования должны применяться с учетом необходимости баланса между задачей расследования преступлений, в том числе совершаемых транснациональными ОПГ, и принципом уважения прав и свобод людей. В большинстве правовых систем действует требование, согласно которому сбор доказательств с помощью таких методов должен осуществляться

при строгом соблюдении ряда гарантий от возможного злоупотребления полномочиями. Кроме того, при расширенном применении специальных методов расследования должна проводиться тщательная проверка собранных с их помощью доказательств, с тем чтобы они отвечали применимым требованиям в отношении доказательств в ходе последующих уголовных разбирательств.

Понятие и виды специальных методов расследования

Какого-либо международного определения понятия «специальные методы расследования» не существует. Конвенция ООН против транснациональной организованной преступности (ТОП), Конвенция ООН о борьбе против незаконного оборота наркотических средств и психотропных веществ 1988 г. и Конвенция ООН против коррупции не содержат соответствующего определения. Предпринимались попытки определить эквивалентное понятие «специальные средства расследования», под которыми понимаются средства или методы, применяемые для сбора доказательств, оперативных данных и информации без ведома лиц, в отношении которых ведется расследование[1].

Следует отметить, что в своей рекомендации Rec (2005) 10 государствам-членам в отношении «специальных методов расследования» особо опасных преступлений, включая акты терроризма, принятой 20 апреля 2005 г., Комитет министров Совета Европы определил «***специальные методы расследования» как методы, применяемые компетентными органами в контексте уголовных расследований для выявления и раскрытия особо опасных преступлений и действий подозреваемых и обеспечивающие сбор информации таким образом, чтобы об этом не знали лица, против которых они направлены***.

В Конвенции ООН против ТОП говорится о надлежащем использовании ***контролируемых поставок*** и предусматривается надлежащее использование других специальных методов расследования по усмотрению компетентных органов государства-участника.

Электронное наблюдение. Электронное наблюдение включает в себя аудио- и визуальное наблюдение, контроль за передвижением и наблюдение за данными[2]. Применение электронных методов сбора доказательств, как правило, регулируется законодательством

---

[1] См.: Council of Europe, *The Deployment of Special Investigative Means* (Belgrade, 2013). P. 12.

[2] *Current Practices in Electronic Surveillance in the Investigation of Serious and Organized Crime* (United Nations publication, Sales No. E.09.XI.19). P. 2.

и в большинстве стран — посредством системы, предусматривающей выдачу ордеров, особенно когда речь идет об электронном наблюдении за частными объектами[1].

Национальные законы по-разному определяют обстоятельства и условия выдачи ордера на электронное наблюдение. Как правило, требуется наличие разумных оснований полагать, что соответствующее преступление было совершено, совершается или будет совершено. К числу других факторов, требующих рассмотрения, относятся серьезность расследуемого преступления, ценность доказательств, которые могут быть получены в ходе наблюдения, наличие альтернативных способов получения искомых доказательств и то, отвечает ли выдача ордера интересам отправления правосудия[2].

Многие нормативные системы содержат специальные положения о действиях в сложных или чрезвычайных обстоятельствах, требующих немедленной организации электронного сбора доказательств или перехвата сообщений. Чрезвычайная ситуация, как правило, связана с наличием серьезной и неминуемой угрозы для национальной безопасности, людей или имущества, но может также включать обстоятельства, при которых без установления наблюдения могут быть утрачены ценные доказательства[3].

Другие формы наблюдения. Другие формы наблюдения включают, с одной стороны, физическое наблюдение и слежение (слежка), которые, как правило, носят менее проникающий характер, чем электронное наблюдение, и предполагают установление физического наблюдения за объектом. С другой стороны, они могут также включать контроль банковских счетов в рамках финансовых расследований.

Агентурные операции и оперативные эксперименты. Как отмечено в документах ООН, ***использование агентов, работающих под прикрытием, которые могут быть участниками общего оперативного эксперимента, имеет большое значение в тех случаях, когда получение информации о деятельности преступников или ОПГ с помощью обычных средств затруднено, и поэтому обусловливает необходимость внедрения агентов в преступные сети или сотрудников, выдающих себя за преступников, в интересах раскрытия преступной деятельности***.

---

1 Sheelagh Brady, "Policing TOC: the national perspective — challenges, strategies, tactics" in International Law and Transnational Organized Crime, Pierre Hauck and Sven Peterke, eds. (Oxford, Oxford University Press, 2016). P. 482.

2 *Current Practices in Electronic Surveillance*. P. 19.

3 Ibid. P. 26.

Доказательства, представленные «осведомителем», будь то сотрудником полиции, работающим под прикрытием, или даже соучастником, могут иметь решающее значение для успеха судебного преследования. Кроме того, под давлением таких неопровержимых доказательств обвиняемые часто предлагают сотрудничество и признают свою вину, что устраняет необходимость в длительных и дорогостоящих судебных процессах (см. также ст. 26 Конвенции ООН против ТОП). Вместе с тем могут возникнуть вопросы о законности использования агентов, работающих под прикрытием, и проведения оперативных экспериментов или допустимости доказательств, собранных с помощью таких средств, в частности ***из-за озабоченности по поводу провоцирования на совершение уголовно наказуемого деяния*** и возможных нарушений прав человека, а также по поводу ресурсов, необходимых для таких операций, и их продолжительности и стоимости.

Использование осведомителей. Использование полицией осведомителей — важная часть работы по расследованию и предупреждению преступлений. Роль осведомителей отличается от роли свидетелей, поскольку они не обязаны давать показания в суде, а в некоторых странах не требуется разглашать информацию о той помощи, которую они оказывают[1].

По определению Совета Европы, ***осведомитель — это лицо, которое устанавливает или поддерживает личные или иные отношения с другим лицом с целью содействия мероприятиям, в рамках которых такие отношения негласно используются для получения информации или доказательств, или для предоставления доступа к любой информации или доказательствам третьему лицу, или для негласного раскрытия информации или доказательств, полученных благодаря использованию таких отношений или в результате их наличия***[2].

В документах ООН подчеркивается, что ***понимание разницы между конфиденциальной и неконфиденциальной информацией и соответствующее обращение с информацией, позволяющей раскрыть личность осведомителей, имеют важное значение, особенно в тех случаях, когда осведомитель тесно связан с преступной деятельностью***. В любом случае следует обращаться к старшему должностному лицу, прокурору или в судебные органы

---

[1] Управление Организации Объединенных Наций по наркотикам и преступности (УНП ООН), «*Рекомендуемые виды практики в области защиты свидетелей при производстве по уголовным делам, касающимся организованной преступности*» (Вена, 2008 г.). С. 22.

[2] Council of Europe, *The Deployment of Special Investigative Means*. P. 43.

за консультацией в отношении использования услуг осведомителей, для того чтобы удостовериться в допустимости собранных с их помощью доказательств. Транснациональный характер многих дел об организованной преступности требует, чтобы следователи были знакомы с законодательством своей страны, а также с законодательством стран, с которыми они сотрудничают.

Методы, применяемые в финансовых расследованиях. Использование финансовых учреждений для выявления подозрительных финансовых операций и их отчетов подразделениям по сбору оперативной финансовой информации позволяет следователям получать информацию о перемещении незаконных средств и их связи с подозреваемыми. В этом контексте использование специальных методов расследования (прослушивание телефонных разговоров, проведение обысков на основании ордеров, опрос свидетелей, обыск и конфискация на основании приказов, истребование материалов и контроль счетов на основании приказов) связано с изучением финансовой документации или доступом к документам, находящимся в распоряжении следователей, обладающих опытом «отслеживания движения денег», сбора деловой и финансовой оперативной информации и выявления сложных незаконных схем и способных принять оперативные меры во избежание исчезновения активов[1].

Методы сбора электронных доказательств

Согласно Справочному документу, подготовленному Секретариатом Конференции участников Конвенции ООН против ТОП, ***«Сбор электронных доказательств и обмен ими»*** (август 2015 г., CTOC/COP/WG.3/2015/2), электронные доказательства могут включать любые созданные или хранимые в цифровой форме данные во всех случаях, когда используется компьютер. К таким данным относится: информация, вносимая ручным способом каким-либо лицом в электронное устройство; информация, вырабатываемая при вычислительной операции или реагировании каким-либо лицом на запрос, когда электронное устройство генерирует информацию в режиме автомата; вырабатываемая и хранимая информация в тех случаях, когда устройство обрабатывает информацию в рамках своей матрицы. Таким образом, ***электронные доказательства представляют собой любую информацию, регистрируемую, генерируемую или хранимую в базах данных, операционных системах, прикладных программах, компьютерных***

[1] Jean-Pierre Brun and others, *Asset Recovery Handbook*: *A Guide for Practitioners* (Washington, D.C., World Bank, 2011). P. 23.

моделях с экстраполированными результатами, электронных и голосовых почтовых сообщениях и даже командах, пребывающих в инертном состоянии в блоках памяти компьютера[1].

Мероприятия для сбора электронных доказательств могут включать в себя: оперативное обеспечение сохранности компьютерных данных; распоряжения о предоставлении хранимых данных о контенте; распоряжения о предоставлении хранимых данных о трафике; распоряжения о предоставлении информации о подписчиках; сбор данных о контенте в реальном времени; сбор данных о трафике в реальном времени; поиск компьютерных аппаратных средств или компьютерных данных; изъятие компьютерных аппаратных средств или компьютерных данных; трансграничный доступ к компьютерной системе или данным; использование средств удаленной технико-криминалистической экспертизы[2].

Сотрудничество правоохранительных органов с другими соответствующими субъектами, в том числе из частного сектора, приобретает в последние годы особенно важное значение для эффективного расследования киберпреступлений и сбора связанных с ними электронных доказательств. В целом поставщики услуг интернета (ПУИ) играют важную роль в обеспечении доступности электронных доказательств.

Учитывая важную роль ПУИ в сборе электронных доказательств, ***Совет Европы принял «Руководящие принципы сотрудничества между правоохранительными органами и поставщиками услуг Интернета в борьбе с киберпреступностью»***. Эти руководящие принципы призваны содействовать выстраиванию надлежащего взаимодействия правоохранительных органов и ПУИ при решении проблем киберпреступности. Данные руководящие принципы являются гибкими и могут применяться в любой стране в соответствии с внутренним законодательством и при соблюдении основополагающих прав граждан. Правоохранительным органам и ПУИ рекомендуется, в частности: участвовать в обмене информацией; содействовать привитию культуры сотрудничества; разработать письменно оформленный порядок взаимодействия;

---

[1] Ireland Law Reform Commission, "Documentary and Electronic Evidence", Consyltation paper, December, 2009. P. 8.

[2] Примеры норм внутреннего законодательства, касающихся этих следственных мероприятий, приведены в разделах Cybercrime Repository (http://cybrepo.unodc.org) SHERLOC (http: sherloc.unodc.org).

рассмотреть возможность установления официальных партнерских отношений; защищать основополагающие права граждан[1].

Электронные доказательства по своей природе являются легко разрушаемыми. При ненадлежащем обращении или изучении они могут быть изменены, повреждены или уничтожены. Поэтому для документирования, сбора, сохранения и анализа такого рода доказательств следует принимать особые меры предосторожности. При несоблюдении таких мер электронные доказательства могут прийти в негодность или могут быть сделаны неверные выводы.

В связи с этим важнейшую роль играет наращивание потенциала на уровне национальных правоохранительных органов и систем уголовного правосудия. ***Оперативные сотрудники правоохранительных органов также испытывают растущую потребность в приобретении и использовании таких базисных навыков, которые используются для составления обоснованного экспертно-криминалистического описания устройств для электронного хранения данных.***

Поскольку при совершении преступлений, сопряженных с электронными доказательствами, широко используются технологические новшества, такие как анонимизирующие сети, криптостойкое шифрование и виртуальные валюты, следователям и оперативным работникам необходимо использовать новые стратегии. Например, активизировать партнерские отношения с научно-исследовательскими группами, которые занимаются разработкой технических методологий в таких областях, как анализ операций с виртуальной валютой[2]. Кроме того, надо учитывать то, каким образом специальные методы расследования, такие как слежка, секретные операции, использование осведомителей и проведение контролируемых поставок в случае продажи запрещенных товаров через интернет, могут использоваться вместе с интернет-расследованиями и методами цифровой криминалистической экспертизы для сбора деликатных и легко разрушаемых электронных доказательств. В целом очевидно, что наращивание потенциала правоохранительных органов и органов уголовного правосудия в области

[1] Guidelines for the cooperation between law enforcement and internet service providers against cybercrime // Council of Europe. URL: https://rm.coe.int/16802fa3ba (дата обращения: 20.08.2021).

[2] См., например: Sarah Meiklejohn and others, “A fistful of bitcoins: characterizing payments among men with no names”, in *Proceedings of the 2013 ACM SIGCOMM conference on Internet measurement conference* (New York, ACM, 2013).

борьбы с киберпреступностью и (или) преступлениями, сопряженными с электронными доказательствами, будет постоянным и непрерывным процессом, учитывая, что продолжают быстро появляться новые технологии и новые методы совершения преступлений[1].

Правовые основы применения специальных методов расследования

Европейский суд по правам человека (ЕСПЧ) отмечал в различных делах, что закон должен быть достаточно четким в своих положениях, чтобы дать людям адекватное представление об обстоятельствах и условиях, при которых государственные органы имеют право прибегать к негласным методам[2].

На основе своих решений в отношении скрытых мер наблюдения ЕСПЧ разработал ***комплекс минимальных гарантий, которые должны быть введены в действие в законодательном порядке во избежание злоупотребления властью***, по следующим позициям: характер преступления, который может послужить основанием для вынесения постановления о наблюдении; категория лиц, к которым могут быть применены такие меры; продолжительность наблюдения; порядок изучения, использования и хранения полученных данных; меры предосторожности, которые должны быть приняты при передаче данных другим сторонам; обстоятельства, при которых записи могут или должны быть стерты или уничтожены. Кроме того, орган, выдающий разрешения, должен быть независимым, и должен быть предусмотрен либо судебный контроль в той или иной форме, либо контроль со стороны независимого органа[3] за деятельностью органа, выдающего разре-

---

[1] Четырнадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию, подготовленный Секретариатом справочный документ к семинару-практикуму 4: Современные тенденции в области преступности, последние изменения и новые решения, в частности использование современных технологий как средства совершения преступлений и инструмента борьбы с преступностью, A/CONF.234/PM.1.

[2] Европейская комиссия по правам человека: дело *Копп против Швейцарии*, п. 64; дело *Хан против Соединенного Королевства*, ходатайство № 35394/97, решение от 12 мая 2000 г., п. 26; дело *Тейлор-Сабори против Соединенного Королевства*, ходатайство № 47114/99, решение от 22 октября 2002 г., п. 18.

[3] Дело *Мейлоун против Соединенного Королевства, п. 67.*

шения[1]. Перехват сообщений, санкционированный только прокуратурой без какой-либо возможности предварительного контроля со стороны судьи, не соответствует требуемым стандартам независимости[2].

В своих решениях, касающихся перехвата сообщений, ЕСПЧ установил, что в законодательном акте, регулирующем негласную деятельность, должны быть предусмотрены следующие ***минимальные гарантии***: определение категорий лиц, телефоны которых могут прослушиваться по судебному постановлению; характер преступления, который может послужить основанием для вынесения такого постановления; ограничение продолжительности прослушивания телефонов; порядок составления отчетов с кратким содержанием перехваченных сообщений; меры предосторожности, которые должны быть приняты с целью передачи записей в целости и сохранности для возможной проверки судьей и защитой; обстоятельства, при которых записи могут или должны быть стерты или уничтожены, в частности, если обвинения были сняты с обвиняемого мировым судьей или он был оправдан судом.

Согласно устоявшейся судебной практике ЕСПЧ ***вмешательство в осуществление прав человека будет считаться необходимым для достижения законной цели***, если оно отвечает так называемой «насущной социальной потребности», в частности, если оно соразмерно преследуемой законной цели и если причины, приводимые национальными властями для ее обоснования, «убедительны и достаточны».

Что касается скрытого наблюдения, то ЕСПЧ констатировал, что национальные власти пользуются довольно широкой свободой усмотрения при выборе средств для достижения законной цели защиты национальной безопасности[3].

«Надлежащее использование специальных методов расследования тесно связано с ***соразмерностью последствий их применения их цели***. Такая соразмерность должна быть проверена

---

[1] Европейская комиссия по правам человека: дело *Юниг против Франции*, ходатайство № 11105/84, решение от 24 апреля 1990 г., п. 33; дело *Аманн против Швейцарии*, ходатайство № 27798/95, решение от 16 февраля 2000 г., п. 60; дело *Иордаки и другие против Молдовы*, ходатайство № 25198/02, решение от 10 февраля 2009 г., п. 40.

[2] Европейская комиссия по правам человека, дело *Думитру Попеску против Румынии* (№ 2), ходатайство № 71525/01, решение от 26 апреля 2007 г., п. 70–73.

[3] Дело *Мейлоун против Великобритании*, п. 81, и дело *Леандер против Швеции*, п. 59.

и обеспечена до применения специальных методов расследования. В связи с этим, принимая решения о применении таких методов, компетентные органы должны провести оценку с учетом тяжести рассматриваемого преступления и определить, является ли оправданным проникающий характер конкретного специального метода расследования.

При оценке соразмерности той или иной негласной меры преследуемой цели необходимо учитывать следующие соображения: соотносится ли серьезность преступления с проникающим характером применяемых специальных методов расследования[1]; имеются ли убедительные и достаточные причины, оправдывающие применение данной меры; можно ли применить менее ограничительную альтернативную меру; соблюдены ли определенные справедливые процессуальные требования в процессе принятия решений; имеются ли достаточные гарантии от злоупотреблений; не подрывает ли проверяемое ограничение саму суть рассматриваемого права[2].

В силу разнообразия специальных методов расследования они могут затрагивать вопросы прав человека на различных уровнях. Например, может быть целесообразным, чтобы контролируемая поставка была санкционирована старшими должностными лицами правоохранительных органов, в то время как электронное наблюдение обычно требует судебного разрешения и надзора. Эксперты ООН рекомендуют к каждому основному виду специальных методов расследования подходить индивидуально, с тем чтобы для каждого из них можно было установить соответствующий режим.

Рекомендация Rec (2005) 10 Комитета министров Совета Европы о «специальных методах расследования» в связи с серьезными преступлениями, включая акты терроризма, — полезный справочный документ для дальнейшего рассмотрения. В ней Комитет министров отмечает необходимость поддержания баланса между обеспечением общественной безопасности посредством правоохранительной деятельности и защитой прав людей. Он также признает, что разработка общих стандартов будет способствовать укреплению доверия общественности к специальным методам расследования.

---

[1] Recommendation Rec (2005) 10 of the Council of Europe Committee of Ministers to member States on “special investigation techniques” in relation to serious crimes including acts of terrorism, appendix, chap. II, para. 5.

[2] См.: Council of Europe, *The Deployment of Special Investigative Means*. P. 17.

Комитет министров устанавливает ряд принципов, которыми государства должны руководствоваться при разработке национальных законов и политики, включая:

— важность надлежащего контроля за применением специальных методов расследования со стороны судебных органов или других независимых органов с помощью системы предварительных разрешений, надзора в ходе расследования или после проверки фактов;

— важность обеспечения соразмерности применяемого специального метода расследования серьезности расследуемого деяния (исходя из того принципа, что должен использоваться наименее проникающий метод, подходящий для достижения поставленной цели);

— необходимость принятия государствами законов, разрешающих представлять в суде доказательства, полученные с помощью специальных методов расследования, при соблюдении права на справедливое судебное разбирательство;

— важность оперативных руководств и обучения специальным методам расследования;

— необходимость того, чтобы государства как можно шире использовали существующие международные договоренности о сотрудничестве между судебными органами и полицией в отношении применения специальных методов расследования, дополняемых при необходимости новыми договоренностями.

Важно, чтобы порядок использования специальных методов расследования подлежал проверке определенного уровня во избежание злоупотребления ими. В разработанных УНП ООН ***Типовых законодательных положениях о борьбе с организованной преступностью*** рекомендуется, чтобы старшее должностное лицо ежегодно направляло парламенту или равнозначному органу доклад о числе запрошенных и выданных разрешений и о числе случаев уголовного преследования, в которых были использованы доказательства или информация, полученные в результате выдачи таких разрешений. В некоторых правовых системах предпочтение может отдаваться дополнительной тщательной проверке посредством, например, направления информации и ее рассмотрения независимым надзорным органом[1].

[1] УНП ООН, *Типовые законодательные положения против организованной преступности* (Вена, 2012 г.). С. 73.

Применение цифровых технологий

Ценным подспорьем в деле устранения угроз, связанных с преступностью, становятся цифровые технологии, которые можно использовать в ходе расследований в качестве инновационных элементов сложных специальных методов расследования. Тем не менее при конкретном применении данных инструментов необходимо проявлять осторожность, чтобы гарантировать их ответственное и этичное использование и избежать нежелательных последствий. Это особенно важно, поскольку многие из нынешних и будущих технологий могут иметь серьезные последствия для неприкосновенности частной жизни и гражданских свобод.

Расширение использования ***биометрических систем и систем сбора данных*** может ослабить действие принципа неприкосновенности частной жизни там, где надлежащий контроль или надзор отсутствует или осуществляется недостаточно строго. Кроме того, сотрудники правоохранительных органов для ускорения процесса идентификации подозреваемых используют ***программное обеспечение для распознавания лиц***. При этом, однако, критики выражают обеспокоенность по поводу того, что эта практика может привести к чрезмерному усилению контроля со стороны правительства, манипуляциям со стороны корпораций и нарушению принципа неприкосновенности частной жизни. Кроме того, способность биометрических систем сохранять данные может поставить под угрозу конфиденциальность ввиду возможности их потенциального неправомерного использования[1].

Для поиска решений в тех случаях, когда есть основания полагать, что применение технологий может войти в противоречие с принципом неприкосновенности частной жизни или другими правами человека, необходим сбалансированный подход. Во избежание использования технологий в качестве троянского коня для потенциального нарушения основополагающих прав необходимо постоянно отслеживать развитие технологий и оценивать его влияние.

В своей резолюции 68/167 о праве на ***неприкосновенность личной жизни в цифровой век Генеральная Ассамблея ООН*** подтвердила право человека на неприкосновенность личной жизни, в соответствии с которым никто не должен подвергаться произвольному и незаконному вмешательству в его личную жизнь. Она

[1] См.: Max Snijder, *Biometrics, Surveillance and Privacy*: *ERNCIP Thematic Group Applied Biometrics for the Security of Critical Infrastructure* (Luxembourg, Publications Office of the European Union, 2016). P. 4.

призвала все государства: провести обзор своих процедур, практики и законодательства, касающихся слежения за сообщениями, их перехвата и сбора личных данных, включая массовое слежение, перехват и сбор, в целях защиты права на неприкосновенность личной жизни путем обеспечения полного и эффективного выполнения всех их обязательств по международному праву прав человека; учредить новые или продолжать использовать уже имеющиеся независимые, эффективные внутренние надзорные механизмы, способные обеспечивать транспарентность в соответствующих случаях и подотчетность в отношении слежения государств за сообщениями, их перехвата и сбора личных данных.

Важным соображением при использовании специальных методов расследования является необходимость ***соблюдения процессуальных гарантий допустимости в суде доказательств, полученных с помощью таких методов, в том числе с использованием цифровых технологий***. В большинстве юрисдикций процесс сбора доказательств требует строгого соблюдения ряда гарантий от возможных злоупотреблений полномочиями, включая судебный или независимый надзор за применением этих методов и соблюдением принципов законности, субсидиарности и соразмерности[1].

В документах ООН отмечено, что допустимость электронных доказательств, в частности, требует соблюдения установленных процедур, гарантирующих права человека (E/CN.15/2018/6, п. 30). При оценке допустимости электронных доказательств особое внимание следует уделять важности соблюдения принципа пропорциональности при использовании специальных методов расследования киберпреступлений, включая использование агентов под прикрытием и удаленной компьютерно-технической экспертизы, особенно в отношении даркнета (UNODC/CCPCJ/EG.2019/2, п. 37).

Кроме того, новой сложной сферой является применение общих принципов внутреннего процессуального законодательства и национальной судебной практики при оценке допустимости доказательств, полученных в ходе судебной экспертизы по делам ***об использовании криптовалют***.

Пункт 1 ст. 20 Конвенции против ТОП не требует от государств-участников принятия мер, обеспечивающих допустимость в суде доказательств, полученных с использованием специальных методов расследования, как это прямо предусмотрено в п. 1 ст. 50 Кон-

[1] Dimosthenis Chrysikos, “Special investigative techniques”, in *The United Nations Convention against Corruption*: *A Commentary*, Cecily Rose, Michael Kubiciel and Oliver Landwehr, eds., Oxford Commentaries on International Law Series (Oxford University Press, 2019). P. 507.

венции против коррупции. Этот элемент относится к позитивному обязательству государства-участника принять законы, правила и процедуры, позволяющие, в целях обеспечения правовой определенности, надлежащего отправления правосудия и защиты прав человека, признать допустимыми в суде доказательства, полученные в результате применения специальных методов расследования.

Несмотря на отсутствие этого элемента в п. 1 ст. 20 Конвенции против ТОП, весьма важно, чтобы ***разработчики национальных законов рассмотрели вопрос о том, можно ли предъявлять в суде доказательства, полученные, например, посредством внедрения или проведения агентурных операций, и если да, то должны ли секретные агенты раскрывать свои подлинные идентификационные данные***. Важно сочетать интересы правосудия (включая необходимость борьбы против транснациональной организованной преступности) с необходимостью обеспечения для обвиняемого справедливого судебного разбирательства[1].

И в Конвенции против ТОП, и в Конвенции против коррупции отсутвуют сведения по вопросу ***о юридической ценности информации, собранной с помощью специальных методов расследования***. Таким образом, решения, касающиеся условий использования такой информации в качестве допустимых доказательств в суде, остаются на усмотрение соответствующего государства и принимаются с учетом основных принципов его правовой системы и методов легализации и удостоверения подлинности, предусмотренных его законодательством.

В своих решениях ЕСПЧ неоднократно отмечал, что допустимость доказательств является в первую очередь вопросом, подлежащим регулированию в соответствии с национальным законодательством. Как правило, оценка представленных доказательств возлагается на национальные суды. Роль ЕСПЧ заключается в изучении вопроса о том, было ли судебное разбирательство в целом, включая способ получения доказательств, справедливым и не привело ли оно к нарушению статьи 6 Европейской конвенции по правам человека.

Применение специальных методов расследования, в частности агентурных операций, само по себе не может являться нарушением п. 1 ст. 6 Европейской конвенции о правах человека, однако они применяются при соблюдении ограничений и гарантий. Что касается ограничений на участие агентов под прикрытием в агентурных операциях, то ЕСПЧ проводит ***четкое различие между***

[1] УНП ООН, *Типовые законодательные положения*. С. 80.

агентом под прикрытием и агентом-провокатором. Деятельность первого ограничивается сбором информации, в то время как второй фактически подстрекает людей к совершению преступного деяния. В деле *Раманаускас против Литвы*[1] ЕСПЧ сформулировал ***понятие провоцирования на совершение уголовно наказуемого деяния*** в нарушение п. 1 ст. 6 указанной Конвенции следующим образом:

«*Подстрекательство со стороны полиции имеет место в тех случаях, когда участвующие в нем сотрудники — будь то сотрудники спецслужб или лица, действующие по их указанию, — не ограничиваются расследованием преступной деятельности в основном пассивным способом, а оказывают на субъекта влияние, подстрекающее его к совершению преступления, которое в противном случае не было бы совершено, с тем чтобы можно было установить факт совершения преступления, т.е. получить доказательства и возбудить уголовное преследование*».

Любая негласная операция должна соответствовать требованию о том, чтобы расследование проводилось «в основном пассивным образом». Если судом будет установлено, что лицо подстрекалось к совершению преступного деяния и доказательства, полученные в результате такого деяния, являются единственными, на основании которых можно сделать вывод о виновности этого лица, то это дает основания для признания факта нарушения права на справедливое судебное разбирательство[2].

К числу соображений, которые необходимо учитывать при установлении того, выходят ли действия агентов под прикрытием за рамки простого пассивного расследования имевшей ранее место преступной деятельности и равнозначны ли они полицейскому подстрекательству, относятся следующие: наличие разумных или веских оснований подозревать, что данное лицо участвовало в предварительных действиях по совершению соответствующего преступного деяния, ранее совершило преступное деяние или имело намерение участвовать в совершении уголовного преступления до установления контактов с ним полицией; начало агентурной операции

---

[1] Европейский суд по правам человека, дело *Раманаускас против Литвы*, № 74420/01, решение от 5 февраля 2008 г.

[2] Европейский суд по правам человека: дело Раманаускас против Литвы, № 74420/01, решение от 5 февраля 2008 г., п. 54; дело *Тейшейра ди Каштру против Португалии*, ходатайство № 25829/24, решение от 9 июня 1998 г., п. 35, 36 и 39; дело *Банникова против России*, ходатайство № 18757/06, решение от 4 ноября 2010 г., п. 34; дело *Балтиньш против Латвии*, ходатайство № 25282/07, решение от 8 января 2013 г., п. 55.

(связано с предыдущим); законность действий агентов под прикрытием; масштабы участия агентов под прикрытием (т.е. они ли были инициаторами установления контакта с данным лицом и проводились ли ранее переговоры или была ли заключена договоренность).

Справочный документ, подготовленный Секретариатом Конференции участников Конвенции против ТОП (июнь 2020 г., CTOC/COP/WG.7/2020/3), «Успешные стратегии применения технических средств, и в том числе информационно-коммуникационных технологий, для предупреждения и расследования случаев незаконного ввоза мигрантов и эффективного реагирования на расширение деятельности преступных групп в киберпространстве», дает наглядный пример ***применения современных технологий для предупреждения незаконного ввоза мигрантов и борьбы с ним.***

Статья 10 Протокола против незаконного ввоза мигрантов по суше, морю и воздуху, дополняющего Конвенцию ООН против ТОП, который вступил в силу 28 января 2004 г., предписывает государствам-участникам обмениваться, согласно их внутренним правовым и административным системам, соответствующей информацией по таким вопросам, как, в частности, техническая информация, полезная для деятельности правоохранительных органов в целях расширения их возможностей по предупреждению, выявлению и расследованию деяний, связанных с незаконным ввозом мигрантов, и уголовному преследованию причастных к ним лиц.

Технические средства применяются правоохранительными органами для выявления лиц, занимающихся незаконным ввозом мигрантов, с помощью компьютерного обучения, систем искусственного интеллекта и распознавания лиц, а также приложений для извлечения данных с целью выявления подозрительных сделок.

Кроме того, технические средства могут облегчать регистрацию, хранение, анализ и обмен информацией, касающейся незаконного ввоза мигрантов. Электронные доказательства, такие как бронирование авиарейсов и банковские записи о снятии наличных денег за рубежом, помогают доказать факт совершения преступлений, связанных с транснациональной преступностью. Для опровержения утверждений о невинной связи и доказательства наличия преступного умысла могут использоваться доказательства того, что подозреваемые применили фальшивые идентификаторы номера звонящего абонента или шпионские программы.

Пограничный контроль. Использование современных технических средств для выявления случаев незаконного пересечения границы принесло заметную пользу в деле охраны границы, цель

которой заключается в предупреждении и пресечении незаконного ввоза мигрантов, как это предусмотрено в ст. 11 Протокола о незаконном ввозе мигрантов, применение которой часто рассматривается в качестве эффективной и практической меры, облегчающей досмотр пассажиров в аэропортах. По имеющимся данным, используется несколько различных технических средств, например ***тепловизионное оборудование*** и другие виды детекторов присутствия человека. Как и все правоохранительные средства, их разработка и использование должны осуществляться с соблюдением норм международного и внутреннего права, в том числе прав человека.

Автоматизированная аппаратура обнаружения. К используемым современным техническим средствам относятся ***рентгеновские и дактилоскопические сканеры, сканеры биометрических паспортов и пользовательские интерфейсы, автоматизированные электронные выходы или входы и биометрические визы***. Одни страны указали на использование широкого спектра устройств, включая ***микроскопы, объективы для распознания невидимых элементов защиты фотографий и устройства для проверки документов, в том числе устройства контроля подлинности и устройства для считывания документов***. Другие страны отметили преимущество использования ***автоматизированных систем установления личности***, т.е. тех из них, которые разрешают пассажирам въезжать в страну на основе распознавания биометрической информации, такой как ***распознавание лица и радужной оболочки глаза***, с тем чтобы избежать ошибок, вызванных человеческим фактором в силу возможной усталости или невнимательности сотрудников службы пограничного контроля. Такие системы могут быть малозатратными, поскольку для их эксплуатации требуется меньше сотрудников.

Например, в Шенгенской зоне в качестве практических инструментов и механизмов выявления незаконного ввоза мигрантов через международные границы внедрены ***Шенгенская информационная система и Визовая информационная система***. Другие конкретные примеры касаются проверки документов в пунктах въезда. Для проверки информации в пунктах въезда используются также базы ***данных Международной организации уголовной полиции (Интерпол)*** и другие системы архивирования изображений, такие как усовершенствованные системы информации о пассажирах. Все эти системы позволяют обмениваться общими элементами данных о пассажирах, желающих совершить поездку, и загружать их. Со-

бранная информация часто используется для ликвидации сетей незаконного ввоза мигрантов.

В настоящее время ведется разработка новых видов технических решений, таких как ***бесконтактное сканирование отпечатков пальцев и лиц, которое позволит в еще большей степени автоматизировать пограничный контроль*** и повысить безопасность. Ожидается, что такие решения приведут к ***созданию так называемой среды «биометрической идентификации по особенностям движения»*** в интересах аэропортов и авиакомпаний, что, в свою очередь, уменьшит время ожидания для пассажиров[1].

Искусственный интеллект. Во всем мире, как и в случае с другими коммерческими приложениями, для незаконного ввоза мигрантов все шире используются вычислительные возможности искусственного интеллекта (ИИ) и компьютерного обучения. ИИ может помочь в составлении прогнозов и рекомендаций или принятии решений на независимой и масштабной основе и без вмешательства человека, ***комбинируя и анализируя оперативные данные из множества источников с помощью запрограммированных алгоритмов***.

В контексте незаконного ввоза мигрантов это, например, включает в себя стратегии использования систем, основанных на ИИ, которые могут помочь в оценке совершающих поездки лиц в пунктах пересечения границы. Подход, основанный на ИИ, позволяет обрабатывать значительный объем данных и обмениваться ими в течение короткого периода времени для проведения всесторонних оценок угроз и оперативного ознакомления с ними других сторон. К примерам применения такого подхода в области пограничного контроля относятся использование алгоритмов, способных распознавать характерные особенности или поведение с использованием данных о совершающих поездки лицах, полученных в прошлом от различных государственных учреждений и из других источников, для проведения математической оценки рисков в режиме реального времени, а также установка камер и радаров высокого разрешения, управляемых с помощью ИИ с использованием спе-

[1] Frontex, “2019 in brief” (January 2020). Фронтекс — Европейское агентство пограничной и береговой охраны, которое собирает и передает информацию о преступности на границах национальным властям и Европолу. Оно сообщило о работе по созданию центрального подразделения Системы авторизации въезда в Европу, а именно новой системы выдачи разрешений на въезд в Европейский союз из стран, для граждан которых въездная виза не требуется. Эта система будет использоваться для проверки заявлений на получение визы.

циального программного обеспечения, которое позволяет отличать необычное передвижение судов от обычного интенсивного морского судоходства[1].

Данные съемки и Глобальной системы определения местоположения. Обнаруживать и идентифицировать подозрительные перемещения на границах и рядом с ними позволяют ***системы слежения на основе данных спутниковой съемки и Глобальной системы определения местоположения***. К числу известных, поставляемых и применяемых видов технического оборудования относятся ***рентгеновские сканеры для автотранспортных средств, тепловизионные сканеры и камеры наблюдения, используемые для обнаружения незаконно ввозимых мигрантов***, в том числе в автотранспортных средствах или в безопасных убежищах, где мигранты могут находиться во время транзита. Такие технические средства и их постепенное совершенствование при условии поддержки со стороны профессионального, хорошо подготовленного персонала могут облегчить организацию более эффективного пограничного контроля и управление миграцией и способствовать этому процессу[2].

На национальном и транснациональном уровнях на практике используются ***комплексные системы наблюдения, способные перехватывать и вести наблюдение за судами в море на большом удалении***, а также определять количество человек на борту. Такие меры могут также облегчить выявление лиц, занимающихся незаконным ввозом мигрантов, которые после перехвата могут попытаться спрятаться среди последних. Для обеспечения возможности обнаружения, распознавания и идентификации на большом расстоянии в качестве ***воздушных платформ для датчиков, таких как оптические камеры в видимом и инфракрасном спектральном диапазонах, все чаще используются беспилотные авиационные системы, включая дистанционно-пилотируемые авиационные системы (ДПАС),*** широко известные как беспилотные летательные аппараты. Кроме того, с помощью ДПАС можно получить полную картину движения судов. Поскольку производство ДПАС, как представляется, находится в постоянном развитии, постепенное снижение стоимости таких технических средств приведет к более широкому их применению.

---

[1] *Koscak P.* Artificial intelligence turns the tide on securing northern border waterways // United States Customs and Border Protection. May 2020.

[2] IOM, Immigration and Border Management. URL: https://www.iom.int/.

Специальные методы расследования в борьбе со смыканием между терроризмом и организованной преступностью

В докладе Совета Безопасности от 29 июля 2020 г. (20-09860 (R) 030820 0308202) «Меры, принятые государствами-членами и структурами Организации Объединенных Наций для решения проблемы смыкания между терроризмом и организованной преступностью» отмечено, что государства — члены ООН приняли меры по активизации сбора и совместного использования оперативной информации, такие как создание или расширение национальных межведомственных оперативных или специализированных координационных центров, занимающихся конкретными вопросами, например вопросами борьбы с терроризмом или с незаконным оборотом наркотических средств. Эти координационные механизмы способствуют расширению сотрудничества и обмену информацией, касающейся терроризма и организованной преступности, и позволяют осуществлять совместный мониторинг и оценку угроз и мер реагирования на них, например проводить ***целенаправленный совместный анализ оперативных данных***, относящихся к торговле людьми и ее взаимосвязанности с терроризмом.

Осуществляется сбор и анализ оперативных данных, включая регулярный анализ объектов, являющихся потенциальными целями террористов, планируются меры противодействия и обеспечивается ***сбор оперативных данных, имеющихся в открытых источниках, таких как социальные сети***. Некоторые государства составили ***списки или разработали базы данных, содержащие информацию о представляющих опасность конкретных группах лиц (таких, как иностранные боевики-террористы и наркоторговцы),*** при помощи которых проводится анализ тенденций и рисков и определяются направления работы следственных органов.

Подчеркивается полезность использования правоохранительными органами оперативных данных для решения проблемы смыкания между терроризмом и организованной преступностью, в том числе данных ***центров анализа оперативной информации***, в работе которых участвуют представители полицейских, разведывательных, пенитенциарных и военных структур. Эти центры занимаются сбором и анализом информации из национальных и международных баз данных, а также оперативных данных, собираемых, в частности, ***с применением специальных методов расследования и с помощью информаторов***. Тогда как некоторые государства сообщили о правовых ограничениях на обмен оперативными данными

между разведывательным сообществом и правоохранительными органами, в других государствах правовые системы поощряют обмен оперативными данными и предусматривают возможность использования таких данных в качестве доказательств в суде.

Во многих государствах подразделения для сбора оперативной финансовой информации собирают, анализируют и распространяют среди правоохранительных органов ***информацию о финансовых операциях, что позволяет последним выявлять закономерности и связи между терроризмом и организованной преступностью***. Для содействия совместному использованию оперативных данных о финансовых операциях могут быть созданы группы по координации, призванные ***снабжать комплексными оперативными данными полицейские и налоговые структуры, занимающиеся особо опасными преступлениями, включая финансирование терроризма***.

Некоторые государства усилили меры безопасности на морских границах и в портах посредством: совершенствования систем пограничного контроля в отношении людей, грузов и багажа в пассажирских и грузовых портовых терминалах; заблаговременной проверки судовой документации до прибытия судов в национальные порты; расширения использования новых технологий в системах управления движением морского транспорта; повышения качества анализа рисков на основе координации действий со структурами разведывательного сообщества и уголовного правосудия; расширения наблюдения за территориальными водами вдоль всего морского побережья.

В качестве одной из основных мер по обеспечению безопасности границ государства-члены выделили внедрение в соответствии с резолюцией 2396 (2017) Совета Безопасности ***систем сбора предварительной информации о пассажирах и данных записей регистрации пассажиров в секторе гражданской авиации***. Эти системы, обслуживаемые специализированными подразделениями, следят за транзитными пассажирами в целях обнаружения и предотвращения перемещения террористов и других преступников, причастных к совершению тяжких преступлений.

Многие государства поощряют тесное взаимодействие между органами финансовой разведки, военными, правоохранительными структурами, прокуратурами, авиационными ведомствами, таможенными властями, береговой охраной, должностными лицами, отвечающими за разработку политики, и субъектами частного сектора как на уровне оперативной деятельности, так и на уровне управления.

В некоторых юрисдикциях ***координация оперативной деятельности осуществляется через целевые группы по специализированным вопросам*** или через совместные следственные группы. Эти группы могут создаваться официально в соответствии с национальными законами и стратегиями, но могут действовать и неофициально. Они способствуют обмену информацией по конкретным делам и разработке стратегий анализа уголовных дел, проведения совместных расследований и судебного преследования.

В целях изучения проблемы смыкания между терроризмом и организованной преступностью государства-члены использовали целый ряд специальных методов, включая ***скрытое наблюдение, прослушивание телефонных разговоров, перехват сообщений и электронное наблюдение***, а также более традиционные методы. Несколько государств отметили, что применение таких методов сопряжено с получением разрешения суда и соблюдением надлежащих юридических процедур и стандартов в области прав человека, что важно с точки зрения ***обеспечения того, чтобы полученная информация была приемлемой для рассмотрения в суде***.

Государства используют ***базы данных по преступности для установления типологий и факторов риска применительно к различным формам терроризма и видам тяжких преступлений*** и опираются на полученную информацию при проведении расследований, при этом одно государство отмечает, что его национальная база данных по делам о терроризме доступна как для национальных, так и для местных органов прокуратуры.

Некоторые государства прибегают к заключению сделок между обвинением и обвиняемыми для получения информации и опираются на обмен такой информацией для ускорения расследований, тогда как другие государства осуществляют судебное преследование по делам о терроризме в соответствии с законами, не имеющими прямого отношения к терроризму, что делается для ***сохранения конфиденциальности источников оперативной информации и секретности***.

В целях создания национального и регионального потенциала для противодействия угрозе смыкания терроризма и организованной преступности многие государства организуют программы подготовки сотрудников. Тематика и содержание учебных мероприятий определяются на основе результатов регулярных оценок потребностей и сосредоточены на таких областях, как ***методы анализа оперативной и другой информации***; отмывание денег и финансирование терроризма, в том числе с использованием виртуальных активов; предупреждение экономических и финансовых

преступлений и борьба с ними; противодействие незаконному обороту наркотиков и торговле людьми; борьба с коррупцией, оказание поддержки жертвам; ***составление психологического портрета террориста***.

Многие государства упомянули о широком двустороннем и региональном обмене разведывательными данными и информацией, в том числе на основе ***соглашений об обмене секретной информацией и о ее взаимной защите***. В некоторых государствах в рамках национальных полицейских структур, разведывательных служб и служб безопасности были созданы ***подразделения, которым поручено осуществлять постоянный мониторинг обмена по международным каналам оперативной информацией*** и информацией по уголовным делам, которая служит ориентиром при анализе разведданных.

Государства отметили, что ***использование баз данных и инструментария Интерпола, включая его уведомления с зеленым или красным углом***, способствует расследованию дел, связанных с организованной преступностью и терроризмом. Государства также упомянули о роли региональных организаций, баз данных и платформ в поддержке международного сотрудничества в области разведки, правоохранительной деятельности и финансов на основе обмена информацией, разработки конкретных и совместных планов действий исходя из выявленных угроз, существующих в регионе.

Кроме того, Интерпол оказывает поддержку национальным правоохранительным организациям в борьбе с иностранными боевиками-террористами и в выявлении их возможных связей с организованной преступностью путем оказания аналитической поддержки в выявлении контактов, в распространении среди сотрудников правоохранительных органов по всему миру, в сотрудничестве с глобальной коалицией по борьбе с организацией «Исламское государство Ирака и Леванта», ***собранных в зонах конфликтов биометрических данных иностранных боевиков-террористов, в обнаружении с использованием баз биометрических данных Интерпола террористов, прибегающих к незаконным путям пересечения границ, и распространении уведомлений с синим углом среди стран, чтобы предупредить их о трансграничном передвижении лиц, подозреваемых в терроризме***.

Всемирная таможенная организация предложила программы обучения по вопросам внедрения передового опыта в области сбора доказательств, делопроизводства, обработки разведывательных данных и использования ***электронных систем регистрации***

данных о конфискациях и предоставила ***оборудование для обнаружения контрабанды***.

Структуры системы ООН в рамках своих соответствующих мандатов также оказывают поддержку государствам-членам в использовании специальных методов расследования против смыкания между терроризмом и организованной преступностью, согласно ***Глобальной контртеррористической стратегии ООН***, положениям соответствующих резолюций Генеральной Ассамблеи и Совета Безопасности.

В интересах выявления и ликвидации связей между терроризмом и организованной преступностью ***УНП ООН продолжало способствовать наращиванию потенциала государств для обмена оперативными данными, сбора и использования электронных данных и данных из открытых источников, применения специальных методов ведения расследований и других оптимальных видов практики в области сбора оперативных данных, относящихся к уголовным делам, и сотрудничества без ущерба для прав человека***.

Контртеррористическое управление ООН приступило к осуществлению новой глобальной программы по оказанию поддержки государствам-членам в создании межучрежденческих координационных механизмов, также известных как ***«координационные ячейки», призванных укрепить национальный межведомственный разведывательный потенциал*** и способствовать сотрудничеству в деле предупреждения, выявления и расследования террористической деятельности и борьбы с ней путем обобщения и анализа информации, в том числе о других особо опасных преступлениях, при соблюдении международных обязательств и стандартов в области прав человека. Стратегическую и техническую поддержку программы обеспечивает ***Отдел полиции ООН.***

Во исполнение резолюций 2462 (2019) и 2482 (2019) Совета Безопасности Контртеррористический центр Контртеррористического управления ООН расширил свою программу по борьбе с финансированием терроризма, которая призвана направлять действия государств, в том числе при помощи ***обновленной технологической платформы, разработанной для оказания поддержки их подразделениям финансовой разведки***. Эта программа, основными партнерами-исполнителями которой являются УНП ООН, Исполнительный директорат Контртеррористического комитета, Интерпол и Управление информационно-коммуникационных технологий, охватывает приоритетные направления работы, непосредственно касающиеся смыкания между терроризмом и транснацио-

нальной организованной преступностью, в частности в виде трансграничной контрабанды наличности и финансовых документов на предъявителя и новейших финансовых технологий, включая мобильные системы обработки платежей, виртуальные активы и формальные и неформальные системы денежных переводов и передачи ценностей.

Контртеррористическое управление приступило к осуществлению ***Программы ООН по борьбе с передвижениями террористов***, направленной на оказание государствам поддержки в наращивании их потенциала для борьбы с передвижениями террористов на основе создания ***групп по сбору предварительной информации о пассажирах и данных записей регистрации пассажиров в секторе гражданской авиации***. Программа осуществляется совместно УНП ООН, Исполнительным директоратом Контртеррористического комитета, Международной организацией гражданской авиации, Управлением информационно-коммуникационных технологий и Интерполом в целях оказания помощи (в настоящее время) государствам в разработке законодательной базы, создании упомянутых групп, установлении связи с перевозчиками и внедрении ***программного обеспечения ООН «goTravel» для оперативной обработки информации о пассажирах и данных записей регистрации пассажиров***. Работа таких подразделений позволяет осуществлять ***картирование и анализ связей между подозреваемыми в терроризме и совершении особо опасных преступлений***. В настоящее время идет работа над расширением Программы, и по завершении этой работы Программа будет включать военно-морской компонент.

Контртеррористическое управление и Контртеррористический центр продолжали оказывать поддержку государствам в укреплении их потенциала ***для предотвращения использования новых технологий в террористических целях, включая кибернетический потенциал, доступ к которому осуществляется через организованные преступные группы, а также по противодействию террористической деятельности и ее расследованию в онлайновом режиме и по сбору цифровых криминалистических доказательств без ущерба для соблюдения прав человека***.

Ю.Н. Жданов, В.С. Овчинский

Стратегия Евросоюза по борьбе с организованной преступностью на 2021–2025 годы и ее значение для совершенствования оперативно-розыскной деятельности в цифровой среде

Как подчеркивается в опубликованной 12 апреля 2021 г. ***Оценке угрозы особо опасной и организованной преступности Европейского союза (2021 EU SOCTA)***, скрытая от общественности из-за непрозрачности своей деятельности организованная преступность представляет собой серьезную угрозу для европейских граждан, бизнеса и государственных институтов, а также для экономики в целом. Организованные преступные группы (ОПГ) присутствуют во всех государствах — членах ЕС. Ландшафт организованной преступности характеризуется сетевой средой, в которой сотрудничество между преступниками является гибким, систематическим и направлено на получение прибыли. ОПГ используют свою крупную незаконную прибыль для проникновения в законную экономику и государственные учреждения, в том числе через коррупцию, подрывая верховенство закона, право людей на безопасность, а также их доверие к государственным властям.

Доходы от преступной деятельности на девяти основных криминальных рынках ЕС в 2019 г. составили 139 млрд евро, что соответствует 1% валового внутреннего продукта Союза.

Около 40% преступных сетей, действующих в ЕС, вовлечены в торговлю нелегальными наркотиками.

Для почти 60% преступных сетей, действующих в ЕС, насилие является частью их криминального бизнеса.

Использование коррупции и злоупотребление законными бизнес-структурами являются ключевыми чертами особо опасной организованной преступности в Европе. Две трети преступников регулярно прибегают к коррупции. Более 80% криминальных сетей используют легальные бизнес-структуры.

Сложность бизнес-модели ОПГ, в частности, была выявлена в 2020 г. в ходе совместного расследования, проведенного французскими и голландскими властями при поддержке Европола

и Евроюста ***в целях ликвидации EncroChat, зашифрованной телефонной сети, широко используемой преступными сетями***. На сегодняшний день дело EncroChat привело к более чем к 1800 арестам и более 1500 новым расследованиям. Кроме того, оно продемонстрировало, насколько широко ОПГ действуют транснационально и онлайн на всех криминальных рынках в сетевой среде, используя все более изощренные методы работы и новые технологии.

В марте 2021 г. еще одна ***совместная операция после взлома Sky ECC***, зашифрованной сети, в которую перебрались многие бывшие пользователи EncroChat, привела к предотвращению более 70 инцидентов с применением насилия, изъятию более 28 тонн наркотических веществ и аресту более 80 подозреваемых в причастности к организованной преступности и незаконному обороту наркотиков в Бельгии и Нидерландах. Было начато более 400 новых расследований в отношении ОПГ высокого риска.

В ЕС растет использование насилия преступниками, причастными к организованной преступности, равно как и угроза насильственных инцидентов из-за частого использования огнестрельного оружия или взрывчатых веществ в общественных местах. Способность ОПГ адаптироваться к изменениям в среде, в которой они действуют, и извлекать из них выгоду, была подтверждена во время пандемии COVID-19.

ОПГ использовали пандемию для расширения преступной деятельности в интернете и для участия в мошенничестве, в том числе с контрафактной медицинской продукцией. Устойчивый высокий спрос на вакцины против COVID-19 делает привлекательным для преступников участие в производстве и поставке поддельных вакцин или в схемах мошенничества, направленных на отдельных лиц или государственные органы. Правительствами ЕС к настоящему времени были выявлены попытки со стороны мошенников продать более 1,1 млрд доз поддельной вакцины на общую сумму более 15,4 млрд евро.

В ходе международной операции при поддержке Европола и Европейского бюро по борьбе с мошенничеством (OLAF) в период с марта по декабрь 2020 г. правоохранительные органы 19 государств-членов и восьми третьих стран изъяли почти 33 млн поддельных медицинских устройств, включая маски для лица, комплекты тестов и диагностики, 8 тонн сырья и 70 тыс. литров гигиенических дезинфицирующих средств.

Экономический кризис, возникший в результате пандемии, увеличивает риски организованной преступной деятельности, которая еще больше проникает в общество и экономику. Транснацио-

нальные угрозы и меняющиеся методы ОПГ, функционирующих в автономном и онлайн-режиме, требуют скоординированных действий, более адресного и адаптированного ответа. В то время как национальные органы власти, действующие на местах, находятся на переднем крае борьбы с организованной преступностью, действия на уровне ЕС и глобальные партнерства имеют первостепенное значение для обеспечения эффективного сотрудничества, а также обмена информацией и знаниями между национальными властями при поддержке общей системы уголовного права и финансовых средств. Кроме того, организованная преступность символизирует связь между внутренней и внешней безопасностью. Для решения этой транснациональной проблемы необходимо ***международное участие в борьбе с организованной преступностью***, включая дальнейшие шаги по развитию партнерских отношений и сотрудничества со странами в непосредственной близости и за их пределами. И Европейский парламент, и Совет отметили, что организованная преступность наносит огромный ущерб, и подчеркнули важность решительных действий ЕС по борьбе со всеми формами организованной преступной деятельности.

14 апреля 2021 г. опубликована ***первая специализированная Стратегия ЕС по борьбе с организованной преступностью с момента вступления в силу Лиссабонского договора***. Эта Стратегия основывается на прошлых достижениях, определяет приоритетные направления работы для лучшей защиты граждан и экономики от ОПГ и предлагает конкретные среднесрочные и долгосрочные действия, которые будут разрабатываться при полном соблюдении основных прав.

Остановимся на важнейших, новаторских положениях Стратегии.

Европейский Союз предоставил правоохранительным органам широкий спектр инструментов для облегчения обмена информацией, которая оказалась критически важной для раскрытия преступной деятельности и сетей. ***Шенгенская информационная система (SIS)*** позволяет оперативным сотрудникам быстро обнаруживать и определять местонахождение лиц и объектов, причастных к организованной преступности, и принимать соответствующие меры. Информация из этой общей базы данных может помочь сотрудникам правоохранительных органов арестовать человека, конфисковать объект или установить передвижения лиц, участвующих в расследовании. Только в 2020 г. поиск в Шенгенской информационной системе проводился почти 4 млрд раз, в ре-

зультате чего было найдено соответствие по более чем 200 тыс. запросов.

Реформа также предоставляет Европолу доступ к оповещениям SIS и обмену дополнительной информацией, а также делает более эффективным использование биометрических данных, вводя возможности использования изображений лиц для целей идентификации и включения профилей ДНК для облегчения идентификации пропавших без вести. Внедрение этих нововведений продвигается полным ходом, так что ***новая система будет полностью готова к работе к концу 2021 г.***

Потенциал SIS в борьбе с организованной преступностью будет дополнительно усилен за счет новой основы для взаимодействия между информационными системами ЕС в области правосудия и внутренних дел. Поставлена задача ***достижения полной функциональной совместимости к концу 2023 г.*** В рамках функциональной совместимости разрабатывается ***функция обнаружения множественных идентификационных данных***, которая путем проверки данных в этих системах поможет эффективно бороться с мошенническим использованием идентификационных данных.

Следователи, работающие изолированно в одном государстве — члене ЕС, часто не могут установить причастность ОПГ к конкретному преступлению. ***Система Prüm 200813*** позволяет правоохранительным органам в ходе своих расследований искать ДНК и отпечатки пальцев в базах данных других государств-членов на основе двусторонних связей, не обнаруживая совпадений, а также осуществлять поиск регистрационных данных автомобиля. Несмотря на то, что система Prüm доказала свою полезность в раскрытии многих преступлений в Европе, ее децентрализованный характер привел к тому, что многие двусторонние связи между национальными базами данных государств-членов не были установлены из-за технической сложности и связанных с этим финансовых проблем. Кроме того, государствам могут потребоваться недели или даже месяцы, чтобы поделиться своими данными о преступлении.

Для повышения эффективности уголовных расследований и усиления автоматизированного обмена информацией о преступниках система Prüm будет модернизирована для удовлетворения оперативных потребностей правоохранительных органов в соответствии с основными правами и требованиями необходимости и соразмерности.

С учетом трансграничного и международного характера организованной преступности информация о поездках имеет суще-

ственное значение для выявления лиц, путешествующих с высокой степенью криминального риска, которые не известны правоохранительным органам, и установления связи между членами ОПГ. ***Обработка данных регистрации пассажиров (PNR)*** помогает соответствующим органам выявлять лиц, причастных к преступной деятельности, совершаемой ОПГ.

Расширенная информация о пассажирах (API), биографические данные пассажиров, собранные авиаперевозчиками во время регистрации, не менее ценны, в том числе из-за их взаимодополняемости с данными из записей регистрации пассажиров.

Одним из ключевых инструментов для реализации Стратегии и активизации усилий против структур организованной преступности посредством скоординированных операций является ***Европейская мультидисциплинарная платформа противодействия угрозе преступности (EMPACT)***. С 2010 г. EMPACT позволяет государствам-членам выявлять приоритетные угрозы преступности в ЕС, для устранения которых необходимы коллективные действия, и решать эти задачи на основе обширного вклада, представленного государствами-членами и другими соответствующими заинтересованными сторонами.

Хотя EMPACT уже дает значительные операционные результаты, например в плане изъятия наркотиков или арестов преступников, в настоящее время он не используется в полной мере. Его сложность, недостаток осведомленности среди непосредственных сотрудников и недостаточное финансирование не всегда обеспечивают заинтересованность и активное участие государств-членов и внешних партнеров, а также препятствуют разработке более сложных операций, которые могут нанести значительный ущерб ОПГ.

Поставлена задача ***укрепить позиции EMPACT в качестве ключевого инструмента ЕС для государств-членов и соответствующих агентств и органов ЕС в целях оперативного сотрудничества в борьбе с организованной и особо опасной международной преступностью***. Это сделало бы EMPACT постоянным вектором структурного сотрудничества между европейскими и национальными стратегиями и действиями по борьбе с преступностью, с согласованной методологией и подходом, в качестве правовой основы для специальных совместных партнерств, основанных на оперативных потребностях.

Комиссия также будет стремиться значительно увеличить финансирование EMPACT, чтобы позволить ему разрабатывать более сложные операции.

Ставится цель повысить роль европейских сетей и экспертных групп в поддержке действий EMPACT.

Стратегия предусматривает ***дальнейшее развитие разведки особо опасной и организованной преступности в Европоле***, а также расширение обмена информацией и следственных действий с третьими странами и регионами, являющимися основными центрами организованной преступности высокого риска, затрагивающей государства — члены ЕС, в том числе через прикомандированных офицеров связи государств-членов.

Интерпол — еще один ключевой участник международного сотрудничества в борьбе с организованной преступностью. ***В 18 базах данных Интерпола содержится более 100 млн записей правоохранительных органов***, в том числе о разыскиваемых преступниках, подозреваемых в терроризме, отпечатках пальцев, украденных автомобилях, украденных и утерянных проездных документах, холодном и огнестрельном оружии. Эти базы данных позволяют правоохранительным и судебным органам выявлять связи и тем самым способствовать расследованию транснациональной организованной преступности.

Основное внимание в расследованиях правоохранительных органов ***нацелено на участников и сети, которые составляют основу криминальных экосистем***. Поскольку большинство преступных организаций структурированы вокруг основной группы, ***ландшафт организованной преступности характеризуется сетевой средой, в которой различные группы и отдельные лица систематически сотрудничают через «совместные предприятия» в рамках рыхлых и подвижных преступных сетей***.

Преступные организации, создающие цепочки поставок на международных криминальных рынках, сотрудничают с более мелкими группами, специализирующимися на определенных видах деятельности, и с лицами, выполняющими ключевые роли, предоставляющими преступникам такие услуги, как подделка документов, юридические консультации, шифрованная связь или транспортировка. Объединяющая способность ОПГ сводит на нет усилия правоохранительных органов, поскольку каждый сегмент криминальной цепочки может быть легко заменен в случае вмешательства правоохранительных органов.

В этой ситуации ставится задача ***активизировать ликвидацию структур организованной преступности, нацелив ее на те ОПГ, которые представляют более высокий риск для безопасности Европы, и на лиц в высших эшелонах преступных организаций***. Для этого некоторые государства-члены создали ***струк-***

туры на национальном уровне или специализированные органы в правоохранительных и судебных органах против мафиозных организаций. Этот опыт оказался эффективным в стимулировании стратегического подхода, поощряющего усилия, ведущие к разрушению криминальной инфраструктуры. Более того, создание специальных полицейских подразделений или судебных органов будет способствовать более широкому трансграничному сотрудничеству.

Комиссия будет способствовать обмену передовым опытом для облегчения тиражирования в государствах-членах таких моделей, адаптированных к национальным особенностям. На европейском уровне оперативное сотрудничество против мафиозных организованных преступных структур, осуществляемое через ***сеть @ ON Network36***, способствует выделению на местах специализированных следователей в государствах-членах для оказания помощи в расследованиях трансграничных ОПГ.

Согласно отчету SOCTA ЕС (2021 г.) 43% ОПГ сформированы вокруг основной группы, 40% — иерархически структурированные, и 17% представляют собой свободные сети. В настоящее время 16 государств-членов участвуют в сети @ON, которая существует с 2014 г. ***Были отобраны 12 особо ценных целей, а именно предполагаемых членов преступных организаций, представляющих особенно высокий риск для двух или более государств-членов.*** Для активизации действий против преступных организаций крайне необходимо дальнейшее структурное сотрудничество. ***Разработка общих критериев для всех государств-членов по определению особо важных целей и содействие оперативному сотрудничеству и обмену информацией в режиме реального времени позволят проводить более систематические расследования в отношении лиц, играющих ключевую роль в преступной сети.***

Больший упор на расследование организованной преступности также требует формирования более надежной разведывательной картины ОПГ, которые находятся в центре сложной сети организованной преступности. Европол и государства-члены должны продолжить свою работу по проведению стратегических и тактических исследований на основе разведывательных данных тех групп, которые представляют большую угрозу безопасности Европы, в том числе путем разработки специальных отчетов, дополняющих Оценку угроз особо опасной и организованной преступности ЕС (SOCTA).

Обмен стратегической информацией с другими участниками, включая миссии и операции Общей политики безопасности и обороны, может быть полезным в этом отношении. Кроме того, необ-

ходим обзор масштабов преступной деятельности и действий, предпринимаемых государствами-членами. Учитывая непрозрачный характер организованной преступности, трудно измерить и количественно оценить эту деятельность, а данные и статистика, доступные Европейскому союзу, фрагментированны и собираются в основном посредством исполнения обязательств по отчетности, разбросанных по различным законодательным актам. Основываясь на результатах уже проведенного всеобъемлющего исследования, Комиссия оценит необходимость более систематического сбора статистических данных в этой области.

Огнестрельное оружие является ключевым фактором роста насилия со стороны ОПГ, позволяя им запугивать своих противников и осуществлять контроль над своими членами и рынками. Чтобы ограничить доступность огнестрельного оружия для преступников, Комиссия приступила к реализации ***нового Плана действий ЕС по борьбе с незаконным оборотом огнестрельного оружия на 2020–2025 годы***.

Незаконный ввоз мигрантов остается ключевым видом деятельности ОПГ. В 2021 г. Комиссия примет ***новый План действий по борьбе с незаконным ввозом мигрантов*** для борьбы с преступными сетями, причастными к этим преступлениям, поддержки правоохранительного и межведомственного сотрудничества и стимулирования сотрудничества с третьими странами, а также с миссиями и операциями Общей политики безопасности и обороны.

Комиссия также предлагает наряду с этой Стратегией ***специальную Стратегию ЕС по борьбе с торговлей людьми на 2021–2025 годы*** для устранения условий этого преступления.

Европейский центр киберпреступности при Европоле (EC3), который был основан в 2013 г., сыграл ключевую роль в отслеживании использования пандемии COVID-19 организованной преступностью, а также в создании информационных материалов и отчетов для информирования государств-членов и общественности, поддержки расследований онлайн-мошенничества, совершаемого ОПГ. Кроме того, он публикует свои регулярные отчеты об оценке угрозы организованной преступности в интернете (IOCTA), которые являются важным источником информации для определения приоритетов в операциях и политике.

В соответствии со Стратегией ЕС 2020 г. по более эффективной борьбе с сексуальным насилием над детьми и Всеобъемлющей стратегией ЕС по правам ребенка (2021–2025) в 2021 г. Комиссия предложит ***закон, совершенствующий защиту детей от сексуального насилия***, в том числе путем требования к соответствующим

поставщикам онлайн-услуг обнаруживать известные материалы о сексуальном насилии над детьми и сообщать об этих материалах государственным органам.

Это обеспечит согласованность с другими законодательными инициативами, в частности с предложением о ***Законе о цифровых услугах***. Комиссия также продолжает поддерживать Европейский парламент и Совет в скорейшем достижении ***соглашения по предложению о регулировании, касающемся добровольных усилий определенных поставщиков услуг в борьбе с сексуальным насилием над детьми в интернете***.

Параллельно Европол поддерживает расширение своей успешной ***кампании «Отслеживание объекта»***, в рамках которой осуществляется сбор информации об отдельных объектах на изображениях, демонстрирующих сексуальное насилие над детьми, что может помочь сузить географическое местоположение насилия и, следовательно, в конечном итоге способствовать идентификации и спасению жертв.

Переход к безналичной экономике, ускоренный пандемией, создал больше возможностей для мошенничества и подделки безналичных платежных средств, таких как кредитные карты и инструменты онлайн-платежей, что представляет серьезную угрозу безопасности ЕС. Европейский союз принял более строгие правила в 2019 г., которые государства-члены должны ввести в действие до 31 мая 2021 г. Комиссия будет внимательно следить за прогрессом, чтобы гарантировать полную эффективность новых правил.

Мошенничество, включая ***махинации с таможенными сборами, акцизами и НДС,*** — это еще одна сфера преступлений. В дополнение к текущим усилиям Европола и Евроюста в этой области будут расследоваться и преследоваться в судебном порядке правонарушения, связанные с участием в преступной организации, если ее преступная деятельность направлена на совершение правонарушений, затрагивающих бюджет Евросоюза, включая особо опасное трансграничное мошенничество с НДС.

Контрафактная продукция составляет 6,8% импорта ЕС и является значительным источником дохода для ОПГ. Медицинские и санитарные товары составляют значительную и растущую долю контрафакции — явления, которое значительно усилилось с пандемией COVID-19. Организованная преступность занимается производством и поставкой поддельных средств защиты, тест-наборов и фармацевтических препаратов, и существует риск того, что ОПГ попытаются использовать возможности, возникающие

в ЕС в связи с высоким спросом на вакцины. Правоохранительные органы совместно с Европолом и Европейским бюро по борьбе с мошенничеством успешно проводят важные операции, ведущие к крупным арестам и изъятию контрафактной продукции, включая медицинские товары, игрушки, продукты питания и напитки.

Во время скоординированной операции Европола, проведенной в сентябре 2020 г., было изъято почти 33 млн поддельных медицинских устройств, связанных с COVID-19, в том числе 8 тонн сырья, масок для лица, тестов и диагностических наборов.

ОПГ все чаще участвуют в таких преступлениях, как ***подделка пестицидов и мошенническое использование органического логотипа ЕС***. Опираясь на свою официальную систему контроля и правоприменения, Комиссия будет продолжать ***наращивать свои усилия по борьбе с продовольственным мошенничеством*** и работать над расширением прав и возможностей национальных властей, формированием политики абсолютной нетерпимости, предотвращения, сдерживания и усилением контроля над преступностью, а также над выработкой эффективных санкций. С этой целью ***в ноябре 2020 г. Комиссия приняла План действий в области интеллектуальной собственности, а в 2022 г. она создаст Набор инструментов ЕС по борьбе с контрафакцией***, в котором будут изложены принципы совместных действий, сотрудничества и обмена данными между правоохранительными органами, правообладателями и посредниками.

Экологические преступления заслуживают особого внимания из-за их пагубного воздействия на биоразнообразие, окружающую среду, здоровье и социальную сплоченность внутри ЕС и в третьих странах. Все виды дикой природы — растения, животные и производные продукты — и домашние животные по-прежнему являются предметом незаконной торговли, часто в больших масштабах, а иногда и с потенциально разрушительными последствиями. ***Незаконное обращение с отходами*** и их перевозки подрывают законную промышленность по уничтожению и переработке отходов. ***Европейский союз принял законодательство, регулирующее законную торговлю дикими животными и отходами,*** и потребовал от государств-членов криминализировать и устанавливать наказания за широкий спектр экологических правонарушений. Эти законодательные инструменты были дополнены ***Планом действий по борьбе с торговлей дикой природой 2016 г. и Планом действий по соблюдению природоохранных требований и управлению 2018 г.***

Европейское бюро по борьбе с мошенничеством значительно расширило свою операционную деятельность по противодействию незаконной торговле товарами, создающими опасность для окружающей среды. Несмотря на эти усилия, контрольные, правоохранительные и судебные органы часто не имеют возможности и ресурсов для эффективного выявления, расследования и преследования экологических преступлений. Это особенно актуально в государствах-членах, где нет специализированных правоохранительных органов или органов прокуратуры и не установлен стратегический подход к борьбе с экологическими преступлениями. Существует необходимость в усилении правоприменительного потенциала на национальном уровне и на уровне ЕС. Налагаемые санкции не обладают достаточным сдерживающим действием, а координация и обмен информацией внутри и между государствами-членами, особенно между административными и правоохранительными органами, недостаточны. Комиссия рассматривает ***Постановление ЕС об отправке отходов и План действий по борьбе с торговлей дикими животными***.

Директива по экологическим преступлениям будет пересмотрена для уточнения объема экологических преступлений, повышения точности применения санкций и содействия использованию эффективных инструментов расследования и обмену информацией. Кроме того, будет расширено сотрудничество через ***европейские сети по защите окружающей среды***. Наконец, поскольку международный аспект незаконного оборота дикой природы имеет решающее значение, Комиссия будет способствовать ***принятию дополнительного протокола в рамках UNTOC***.

Незаконный оборот культурных ценностей оказывает разрушительное воздействие на культурное наследие стран, предоставляет средства для финансирования преступных организаций и играет важную роль в отмывании денег. ***Быстрое взаимодействие с археологами и историками искусства может в значительной степени способствовать расследованию незаконного оборота культурных ценностей.***

Для борьбы с этой уникальной формой преступности Комиссия продолжит оказывать поддержку ***наращиванию потенциала среди экспертов по культурному наследию***, включая сеть таких экспертов, которых государства-члены могут использовать в рамках EMPACT. Их структурированное сотрудничество с правоохранительными органами будет поддерживаться с целью облегчения расследований, а также финансирования проектов по противодействию незаконному обороту культурных ценностей. Более того, Комиссия

рассмотрит другие необходимые меры по борьбе с этим явлением, в том числе посредством улучшения возможности отслеживания культурных ценностей в режиме онлайн и офлайн на внутреннем рынке, сотрудничества с третьими странами, в которых происходит разграбление культурных ценностей. С этой целью Комиссия предложит ***План действий по борьбе с незаконной торговлей культурными товарами в 2022 году***.

Организованная преступность в ЕС в основном зависит от способности отмывать огромные суммы преступных доходов. В то время как три четверти преступных организаций попрежнему используют основные методы для сокрытия своих незаконных доходов, такие как инвестирование в недвижимость или другие дорогостоящие товары, другие полагаются на все более изощренные методы, реализуемые с помощью «белых воротничков», занимающихся отмыванием денег. Финансовый след, который преступники оставляют после себя, является ключевым показателем их деятельности, обеспечивая следователям полезные зацепки и бесценные доказательства для обвинения преступников. Таким образом, ***борьба с преступными финансами имеет решающее значение для раскрытия преступной деятельности, сдерживания преступности и предотвращения проникновения в легальную экономику и общество***. Несмотря на развитие законодательной базы по борьбе с отмыванием денег и возвращением активов, выявляется лишь незначительная доля операций по отмыванию денег и ***конфискуется только 1% криминальных активов***. Это усугубляется широким использованием финансовых каналов с более ограниченным надзором, чем банковский сектор, таких как ***виртуальные валюты***.

Как подчеркивается в ***Плане действий по борьбе с отмыванием денег на 2020 год***, нормы ЕС по борьбе с отмыванием денег должны быть значительно улучшены, чтобы устранить серьезные расхождения в способах ее применения и серьезные недостатки в обеспечении соблюдения правил. Финансовые расследования не используются в полной мере, отчасти из-за недостаточного потенциала правоохранительных органов для проведения этих сложных и обременительных расследований. Кроме того, возможности лишить преступников их активов, полученных незаконным путем, еще больше препятствует узкая сфера применения правовых рамок конфискации с точки зрения охватываемых активов и преступной деятельности.

Более того, подразделения по возврату активов в настоящее время сталкиваются с проблемами при отслеживании активов,

поскольку они не имеют, например, полномочия на временное замораживание с целью предотвращения распыления активов или прямого и немедленного доступа к определенным публичным реестрам, таким как центральные земельные реестры или реестры центральных компаний. Более того, возвращенные активы также не всегда управляются эффективно и недостаточно используются для выплаты компенсаций жертвам или на благо общества.

Как было объявлено в Плане действий по борьбе с отмыванием денег на 2020 год, обеспечение эффективной реализации существующей системы борьбы с отмыванием денег является приоритетной задачей. В дополнение к текущим усилиям по обеспечению надлежащей реализации Комиссия готовит законодательные предложения, направленные на усиление и ***развитие Рамочной основы ЕС по борьбе с отмыванием денег, предлагая во втором квартале 2021 г. создать единый свод правил прямого действия: усилить надзор на уровне ЕС и создать механизм ЕС для координации и поддержки подразделений финансовой разведки***. В равной степени необходимо и дальше развивать культуру ранних финансовых расследований во всех государствах-членах и наращивать потенциал следователей по борьбе с финансовыми аспектами организованной преступности.

Создав ***Европейский центр по финансовым и экономическим преступлениям***, Европол расширил свои возможности по поддержке государств-членов в проведении финансовых расследований. Ставится задача активизировать усилия по замораживанию и конфискации через дальнейшее усиление правовой базы на уровне ЕС и усиление операционных возможностей офисов по возвращению активов.

Чтобы обеспечить более строгий режим конфискации и предоставить национальным отделам по возвращению активов более эффективные полномочия, Комиссия предложила ***в 2022 г. пересмотреть Директиву о конфискации 2014 г. и Решение Совета 2007 г. о бюро по возвращению активов***, чтобы: увеличить охват уголовных преступлений; ввести более эффективные правила конфискации без вынесения обвинительного приговора; обеспечить эффективное управление, социальное повторное использование конфискованных активов и компенсацию жертвам преступлений, а также укрепить способность подразделений по возвращению активов отслеживать и идентифицировать незаконные активы.

Кроме того, Комиссия рассмотрит возможные варианты, касающиеся системы начальных финансовых расследований и финансовых расследований после вынесения приговора. Быстрый

доступ к финансовой информации необходим для проведения эффективных финансовых расследований, а также для успешного отслеживания и конфискации активов. Поэтому первостепенное значение имеет своевременное применение государствами — членами ЕС ***Директивы об облегчении доступа к финансовой информации***, которая предоставляет правоохранительным органам доступ к централизованным реестрам банковских счетов и укрепляет сотрудничество между правоохранительными органами и подразделениями финансовой разведки. Комиссия также пересмотрит Директиву, чтобы предоставить правоохранительным органам ***доступ к будущей платформе, объединяющей реестры банковских счетов по всему Евросоюзу***.

Одновременно необходимо будет улучшить международное сотрудничество в борьбе с отмыванием денег. Государства-члены должны в полной мере использовать возможности, предлагаемые ***Оперативной сетью по борьбе с отмыванием денег (AMON), неформальной международной сетью правоохранительных органов по борьбе с отмыванием денег, и Межведомственной сетью Camden Asset Recovery (CARIN), неформальной сетью практикующих сотрудников правоохранительных и судебных органов***, специализирующихся в области отслеживания, замораживания, ареста и конфискации активов.

Согласно действующим антикоррупционным правилам ЕС государства-члены обязаны ***криминализировать как активную, так и пассивную коррупцию государственных должностных лиц***, установить адекватные санкции и обеспечить привлечение к уголовной ответственности предпринимателей, коррумпирующих чиновников. Однако эти инструменты не охватывают определенные преступления, связанные с коррупцией, такие как злоупотребление влиянием, злоупотребление властью, незаконное обогащение, незаконное присвоение или иное нецелевое использование собственности государственным должностным лицом. Совсем недавно Евросоюз принял ***новое законодательство, защищающее информаторов*** и требующее создания безопасных каналов для сообщения о коррупционных действиях.

Предполагается усилить потенциал национальных властей по расследованию особо сложных дел о коррупции, связанных с организованной преступностью, в частности, путем ***создания специализированных антикоррупционных структур***.

Кроме того, учитывая решающую роль СМИ в раскрытии дел о коррупции, чрезвычайно важно обеспечить безопасность журналистов-расследователей по всему Евросоюзу, в том числе защиту

от неправомерных судебных разбирательств. Как заявлено в Плане действий европейской демократии, ***в 2021 г. Комиссия выпустит Рекомендацию о безопасности журналистов и выдвинет инициативу по борьбе с судебными исками о злоупотреблениях против журналистов и правозащитников***.

Из-за экономической ситуации, вызванной пандемией COVID-19, существует повышенный риск того, что ***организованная преступность захватит ослабленные компании и проникнет в целые секторы бизнеса***. Уже есть доказательства преступных попыток обмана различных финансовых механизмов, созданных для поддержки восстановления экономики.

Чтобы противостоять этой угрозе и определить ключевые точки для вмешательства и повышения осведомленности, государствам-членам и Европолу необходимо ***составить оперативную картину о масштабах и степени криминальных инвестиций, методах проникновения и секторах, подверженных риску***.

Ставится цель укрепить сотрудничество правоохранительных органов с гражданским обществом. Необходимо использовать административные инструменты, такие как процедуры получения разрешений, тендеры и субсидии, для предотвращения проникновения организованной преступности в легальный бизнес и административную инфраструктуру.

Местные власти должны быть уполномочены при полном соблюдении основных прав устанавливать барьеры, которые защищают «экономическую ткань» от организованной преступности. Местный аспект также играет ключевую роль в сокращении возможностей для пополнения криминальными группами своих рядов. Лица, выросшие в среде организованной преступности и в неблагополучных с социальной и экономической точки зрения районах, наиболее уязвимы для вербовки в целях преступной деятельности. Начиная с мелких преступлений или второстепенных ролей в организации, они станут членами и лидерами преступных организаций завтрашнего дня. Целенаправленные действия в окрестностях и общинах оказались успешными в плане предложения альтернатив, которые не позволяют молодым людям присоединиться к жизни, полной насилия и преступности. Более того, мероприятия по предупреждению преступности, такие как ***общественная полиция или кампании по повышению осведомленности в районах***, особенно затронутых преступной деятельностью, имеют важное значение для повышения устойчивости общества к деятельности ОПГ.

Поиск доказательств, включая законный доступ к коммуникационным данным, является краеугольным камнем расследо-

ваний и судебных преследований правоохранительных органов, которые привлекают преступников к ответственности. Поскольку наша жизнь и деятельность более, чем когда-либо, сместились в интернет, ***следы преступности также стали цифровыми***. Организованная преступность планируется, осуществляется и скрывается в интернете, продает запрещенные вещества и продукты и находит оригинальные способы отмывания прибыли, не ограничиваясь физическими границами. Масштаб проблемы усугубляется быстро развивающимися технологиями.

Перенос доказательств из физического в онлайн-пространство создает множество проблем, включая скорость, с которой данные могут быть перемещены между юрисдикциями, или возможность «спрятаться» за шифрованием. Кроме того, некоторые инструменты и меры для сбора вещественных доказательств еще не полностью адаптированы к цифровому миру. Это может затруднить или замедлить уголовное расследование и судебное преследование, поскольку данные недоступны или доступны несвоевременно. Для расследования организованной преступности обычно требуется доступ к данным электронных коммуникаций, чтобы установить связь между преступлением, преступником и жертвами, а также для отслеживания преступных сетей. Эти коммуникации, учитывая масштаб и структуру сети организованной преступности, правоохранительным органам сложно отследить без ретроспективного доступа к метаданным связи.

«Отсутствие таких данных делает особенно трудным выявление центральных действующих лиц, дергающих за ниточки в фоновом режиме». Таким образом, идентификация и арест часто затрагивают только самые низкие уровни этих сетей, тех, кто был на месте преступления, а не центральных действующих лиц.

Для обеспечения доступа к цифровым доказательствам и следствию государства-члены создали механизмы хранения данных. Учитывая принцип конфиденциальности электронных сообщений, поставщики услуг связи могли стереть метаданные к тому моменту, когда правоохранительные органы запросили доступ к ним. В таких случаях важные доказательства могут быть потеряны, если только провайдеры не обязаны по закону хранить коммуникационные метаданные в течение разумно более длительного периода в соответствии с законодательной базой хранения данных. Это может привести к тому, что преступления не будут успешно расследованы или потерпевшие не будут идентифицированы. Метаданные связи имеют, например, особое значение при расследовании и судебном преследовании киберпреступлений, часто являются главным сред-

ством обнаружения преступления и выступают в качестве основных доказательств. Они также могут быть важным средством подтверждения (или опровержения) других типов доказательств, относящихся к фактам дела.

В то же время в связи с реализацией мер по сохранению данных требуют решения важные вопросы, касающиеся вмешательства в основные права, включая право на неприкосновенность частной жизни и защиту личных данных. В своих недавних постановлениях о хранении данных ***Суд Европейского Союза подтвердил свою предыдущую судебную практику, согласно которой данные электронных коммуникаций являются конфиденциальными и, в принципе, данные о трафике и местоположении не могут храниться в общем и неизбирательном порядке***. Объем мер по хранению данных может быть оправдан только в связи с их вмешательством в основные права, когда они необходимы и соразмерны преследуемой цели. Суд установил ограниченные исключения из этого правила, касающиеся национальной безопасности, общественной обороны и безопасности или предотвращения, расследования, обнаружения и судебного преследования.

Комиссия проанализирует и наметит возможные подходы и решения в соответствии с постановлениями Суда, которые отвечают потребностям правоохранительных и судебных органов, таким образом, чтобы это было оперативно полезным, технически возможным и юридически обоснованным.

Эффективное реагирование правоохранительных органов также требует своевременного доступа к цифровым доказательствам, если они находятся у поставщиков в другой юрисдикции. В 2018 г. Комиссия предложила пакет доказательств для облегчения доступа к электронным доказательствам через границы на основе европейских постановлений о производстве и сохранности. Европейский парламент и Совет в настоящее время участвуют в межведомственных обсуждениях при поддержке Комиссии, чтобы найти необходимые точки соприкосновения, ведущие к быстрому принятию этих предложений. Более того, в рамках усилий по ускорению цифровизации правоохранительной и судебной системы все государства-члены должны участвовать ***в Системе цифрового обмена электронными доказательствами (eEDES)***. Параллельно необходим быстрый прогресс в многосторонних и двусторонних международных переговорах для облегчения сотрудничества с международными партнерами и установления совместимых правил на международном уровне для трансграничного доступа к электронным доказательствам.

Шифрование необходимо в цифровом мире, поскольку оно обеспечивает безопасность цифровых систем и транзакций, а также защищает ряд основных прав, включая свободу выражения мнений, конфиденциальность и защиту данных. Однако, если шифрование используется в преступных целях, оно скрывает личность преступников и скрывает содержание их сообщений. Комиссия предложила ***набор из шести практических мер для поддержки правоохранительных и судебных органов, когда они сталкиваются с шифрованием данных, хранящихся на устройствах (например, телефонах или жестких дисках), в ходе уголовных расследований, без запрета, ограничения или ослабления шифрования***. В рамках этих мер новое средство дешифрования Европола, запущенное Комиссией в декабре 2020 г., будет способствовать решению этих проблем. ***Европейская группа по обучению и образованию в области киберпреступности (ECTEG)*** разработала учебные модули и провела пилотные курсы. Эти курсы будут включены в программу регулярного обучения ***Европейского полицейского колледжа (CEPOL)***.

Помимо обычных устройств, существует нишевый рынок устройств для зашифрованной связи, которые также приобретаются и используются ОПГ.

Как показали недавние операции *Encrochat* и *Sky ECC*, правоохранительным органам ЕС необходимо постоянно наращивать свой потенциал по работе с зашифрованной информацией в контексте уголовных расследований в соответствии с действующим законодательством.

В декабре 2020 г. Совет принял резолюцию, в которой содержится призыв к активному обсуждению с технологической отраслью и разработке соответствующей нормативной базы, которая позволила бы национальным властям эффективно выполнять свои оперативные задачи, одновременно защищая конфиденциальность, основные права и безопасность связи. Кроме того, Совет попросил улучшить координацию усилий государств-членов и институтов и органов Европейского союза. Как объявлено в ***Программе борьбы с терроризмом***, Комиссия работает над определением технических, операционных и юридических решений для обеспечения законного доступа к зашифрованной информации при сохранении эффективности шифрования для защиты конфиденциальности и безопасности сообщений.

В 2020 г. Комиссия вместе с технологической отраслью, экспертами по криптографии, членами организаций гражданского общества и компетентными органами провела экспертный процесс

для определения технических решений, которые могут помочь компаниям конкретно обнаруживать сексуальное насилие над детьми в конечном итоге.

Комиссия будет поддерживать исследования, чтобы определить, какие технические решения являются наиболее осуществимыми и могут быть расширены и реализованы на законных основаниях для компаний. В более широком смысле, Комиссия будет управлять процессом анализа с соответствующими заинтересованными сторонами существующих возможностей и подходов для законного и целевого доступа к зашифрованной информации в контексте уголовных расследований и судебного преследования. Эти подходы не должны приводить к общему ослаблению шифрования или к неизбирательному наблюдению. Данный анализ будет не только сосредоточен на устранении текущих препятствий, но также будет охватывать прогноз вероятного развития технологий шифрования и дешифрования и необходимое сотрудничество с академическими кругами и частным сектором с этой целью.

Кроме того, Комиссия активизирует свои усилия в области стандартизации для поддержания возможностей ***законного перехвата в контексте 5G и за его пределами***. В результате этого процесса Комиссия предложит дальнейшие шаги в 2022 г. для решения ***проблемы законного и целевого доступа к зашифрованной информации в контексте уголовных расследований и судебного преследования***, которые будут основаны на тщательном отображении того, как государства-члены обращаются с шифрованием.

Правоохранительным органам и судебным органам необходимо идти в ногу с быстро развивающимися технологиями, используемыми преступниками в их трансграничной деятельности. Это требует координации в разработке инструментов и тренингов между государствами-членами и между секторами в таких областях, как ***цифровая криминалистика, разведка с открытым исходным кодом, криптовалюты, расследования в даркнете***, например, чтобы получить доступ и, где возможно, закрыть форумы, торгующие незаконными товарами и услугами.

Существующие механизмы ЕС (EMPACT, агентства ЕС, такие как Европол, CEPOL и Евроюст, сети практиков, программы финансирования, такие как Фонд внутренней безопасности) могут сыграть ключевую роль в содействии более эффективному подходу к онлайн-расследованиям за счет скоординированных и целенаправленных действий по развитию способностей и компетенций. Потребности онлайн-исследователей должны быть достоверно определены. Европол, в соответствии со своим мандатом, и ***Инно-***

вационный центр ЕС в области безопасности должны координировать всесторонний анализ технологических пробелов и потребностей в области цифровых расследований, а также прогнозный анализ, который играет важную роль в управлении программами исследований, инноваций и развития, и инструменты политики, способствующие наращиванию потенциала.

Важно, чтобы соответствующие организации и сети поддерживали эту работу. Исходя из этого, Европол и Инновационный центр ЕС в области безопасности должны установить приоритеты для исследований и разработок, которые будут утверждены государствами-членами.

Исследования и инновации необходимы как для разработки и корректировки технологий для расследований, так и для борьбы с преступностью, которой способствуют технологии. ***Программа ЕС по исследованиям и инновациям Horizon 2020*** профинансировала разработку инновационных технологических решений для повышения потенциала национальных властей в борьбе с организованной преступностью. Эта работа будет дополнительно усилена ***новой программой Horizon Europe***, которая будет финансировать исследовательские проекты для улучшения разведывательной картины об организованной преступности, разрабатывать инструменты и учебные программы, а также укреплять межведомственное сотрудничество. Комиссия будет способствовать доступу к высококачественным наборам данных, необходимым для разработки инструментов расследования, включая системы искусственного интеллекта (ИИ), которые отвечают потребностям правоохранительных органов в уголовных расследованиях, например, для анализа больших объемов данных или расследований в даркнете.

С этой целью Комиссия поддержит ***в рамках программы DIGITAL создание Европейского пространства данных безопасности***, которое будет использовать ***Инновационный центр ЕС по внутренней безопасности*** — это совместная сеть для поддержки инновационных лабораторий агентств ЕС.

В Рабочей программе DIGITAL на 2021–2022 гг. есть положение по созданию ***основы архитектуры федеративных данных для инноваций в области безопасности путем финансирования создания национальных компонентов Европейского пространства данных безопасности для инноваций***. Это позволит внедрять инновации и обеспечивать развитие за счет создания экосистемы в масштабах ЕС для обмена, разработки, тестирования, обучения и проверки алгоритмов для инструментов ИИ для правоохрани-

тельных органов и оценки инструментов для правоохранительных органов.

Кроме того, Комиссия будет поддерживать государства-члены в отношении пилотных проектов по решениям в области ИИ, которые помогут стимулировать внедрение инноваций со стороны правоохранительного сообщества. Правоохранительные органы, промышленность и научные круги должны сотрудничать в сети, поддерживаемой финансированием ЕС, для разработки инструментов и решений на уровне ЕС, которые отвечают потребностям правоохранительных органов ЕС, таким образом поддерживая работу Европола по предоставлению услуг и технических решений правоохранительным органам ЕС. Эта сеть призвана обеспечить устойчивость проектов Horizon Europe и Фонда внутренней безопасности и поддержать Европол в этих усилиях. Сеть должна бесплатно доставлять свои результаты через Европол правоохранительным органам и постоянно совершенствовать существующие решения. С этой целью ***Европол должен стать универсальным центром для предоставления доступа к инструментам и услугам, таким как анализ вредоносных программ, национальным правоохранительным органам***.

Хотя исследование и анализ цифровых доказательств лежат в основе большинства расследований, уровень необходимых навыков в области уголовного судопроизводства, тактики и методов цифрового расследования или цифровой криминалистики все еще недостаточен. Кроме того, доступ к передовым оперативным знаниям в конкретных областях, таких как судебная экспертиза «Интернета вещей», остается проблемой для ряда государств-членов. Развитие обучения должно основываться на определении компетенций, необходимых для проведения цифровых расследований, и связанных профессиональных профилей (например, ***аналитик данных, онлайн-следователь или цифровой судебно-медицинский эксперт***). С этой целью Европол и CEPOL должны работать с государствами-членами над определением и периодическим обновлением ***«Структуры профессиональных компетенций»***. Исходя из этого, Европейская комиссия должна поддерживать разработку учебных материалов через ***Европейскую группу по обучению и образованию в области киберпреступности (ECTEG)*** и поддерживать проведение обучения на национальном уровне с помощью имеющихся инструментов.

CEPOL и ***Европейская сеть обучения судей (EJTN)*** должны регулярно оценивать потребности в обучении и соответственно определять приоритеты его проведения, в том числе для дальней-

шего развития и обеспечения безопасности на основе различных типов наборов данных.

Основываясь на структуре компетенций обучения, CEPOL должен также тесно сотрудничать с практиками и государствами-членами для создания ***схем сертификации/аккредитации для экспертов по цифровым расследованиям***. Такие схемы могут способствовать:

— увеличению количества экспертов, способных проводить тренинги в определенных областях;

— приграничному сотрудничеству, поскольку сертификация/аккредитация предоставит гарантии относительно сбора и обработки доказательств, обеспечивая их допустимость в суде также в других юрисдикциях;

— выявлению специализированных следователей.

Цифровые расследования могут потребовать опыта, который в ЕС весьма ограничен, например, в отношении криптовалют, программ-вымогателей или расследований в дарквебе. Государства-члены должны определить экспертов, которые развили передовые навыки в этих областях, чтобы поддерживать друг друга в операциях, где такие знания необходимы. Комиссия будет поддерживать Европол в создании механизмов, гарантирующих, что органы власти и эксперты государств-членов будут иметь надлежащие стимулы для того, чтобы стать частью группы экспертов.

* * *

Как можно было убедиться, Стратегия ЕС по борьбе с организованной преступностью носит многофункциональный характер, с акцентом на деятельности правоохранительных органов в цифровом мире. Ее положения заслуживают внимательного изучения и для развития теории и практики оперативно-розыскной деятельности по борьбе с организованной преступностью в нашей стране.

И.Ю. Сундиев

Развитие насыщающего террора в форме скулшутинга и задачи оперативных подразделений

В периодичности таких происшествий, как случившаяся 11 мая 2021 г. трагедия в Казани, нет жесткой закономерности. ***Скулшутинг (вооруженные нападения на школу)*** — глобальное явление. Количество инцидентов со стрельбой во всем мире достаточно велико. При этом в период пандемии и локдаунов очень серьезные патопсихологические изменения произошли у всех групп населения, и у подростков в том числе. Но если раньше подобные отклонения у молодых людей можно было выявить на более или менее ранней стадии и благополучно нейтрализовать, то сейчас, к сожалению, количество неучтенных случаев достаточно велико.

В новом полузакрытом мире подростки живут в Сети, для них ничего более реального больше не существует. Наибольшее влияние на молодежь имеют не те живые люди, которые их окружают, а именно цифросетевые ресурсы. На тех, что действуют на территории нашей страны, за последние два года значительно увеличилось число сетевых сообществ, посвященных скулшутингу. А это инструмент формирования так называемого ***насыщающего террора***[1]***, который должен вызвать страх, ужас и всевозможное недовольство населения***.

Казанский стрелок Ильназ Галявиев назвал себя богом и призвал к уничтожению «биомусора» в Telegram-канале. Но проблема не конкретно в этом ресурсе. Это явление развивается практически в любых цифровых сетях. Тематика скулшутинга, после того как у нас были приняты соответствующие нормативные документы, почти полностью ушла из «VK» в мессенджеры — в *Telegram*, *WhatsApp* и *TikTok*.

Как ни странно, на первом месте по количеству материалов, которые «отзываются» на хештеги, связанные с тематикой скулшутинга (таких как *Колумбайн*, *Естественный отбор*, *Natural*

[1] Насыщающий террор — модерация через цифросетевые ресурсы регулярных и географически разнесенных террористических акций против мирного населения, широко освещаемых в традиционных и новых медиа.

selection, *Wrath*, *Гнев*, *Ненависть*, *Убийцы*, *Эрик Харрис*, *Дилан Клиболд*, *Дилан Руф*, *Владислав Росляков*, *Columbine*), стоит «TikTok». Мы всегда относились к нему как к детской, т.е. безобидной, сети. Но в последнее время там наблюдается резкий всплеск количества публикаций о скулшутинге — речь идет практически о пособиях. Размещают объявления о покупке униформы, всевозможные рассуждения о том, как можно убить максимальное число людей и тому подобные вещи. То есть огромное количество материалов направлено на деструкцию молодых людей.

Что делать с такими мессенджерами? Первое и самое главное — четко понять гиперактуальность проблемы насыщающего террора, который призван разрушить наше государство. К этому так и надо относиться. Это не детские игрушки, не проявление психологических отклонений у одного-двух персонажей, а достаточно массовое явление. Аудитория колумбайн-сообществ в различных сетях и мессенджерах — это многие десятки тысяч подростков[1].

В телевизионных ток-шоу можно услышать, мол, вот, подумаешь, дети обсуждают всякие темы, зато выплескивают агрессию и больше никого не убивают. Но когда несколько десятков тысяч молодых людей говорят о том, какими способами они будут убивать, — это явный сигнал о том, что они готовы перейти от слов к реальным убийствам.

Безусловно, в зоне высокого риска находятся все школы и колледжи именно в силу возраста и общей невротизации учеников. В вуз человек, как правило, приходит уже с другими целями и мотивами, поэтому не склонен к такого рода действиям, и, насколько я знаю, в мире не зафиксировано массовых расстрелов в университетах. А что касается школ, то часто агрессия юных террористов выливается именно на те учреждения, где они раньше учились. Причина состоит в том, что обиды у патологически невротизированных молодых людей приобретают гиперзначение, и возможность ответить за причиненную боль становится целью жизни. Цифросетевые сообщества колумбайнеров подсказывают и показывают решение — убить обидчиков, всех. При этом обзывать жертвы «биомусором» — классика жанра, ведь уничтожать мусор — это благородная цель, возвышающая убийцу в собственных глазах.

Подростки, которые интересуются этой темой, должны четко понимать: они не играют, а попадают в категорию особо опасных

[1] *Ашманов И., Касперская Н.* Методическое пособие по выявлению признаков риска поведения в социальных медиа. М.: Крибрум, 2019. URL: https://www.kribrum.ru/monitoring/

преступников, террористов. И в данном случае персонаж, который называет себя богом, должен отвечать за совершение теракта. Если мы таким образом — достаточно жестко — будем расценивать каждый подобный случай, это убавит прыти у молодых людей.

На мой взгляд, убийство нескольких человек в казанской гимназии, совершенное с заранее определенным замыслом, со всеми признаками организации, — это террористическое преступление.

Скулшутинг отвечает всем признакам террористической деятельности, в частности предусматривает:

а) организацию, планирование, подготовку, финансирование и реализацию террористического акта (расстрела или иного способа массового убийства учеников, учителей и работников школы);

б) подстрекательство к массовому убийству;

в) организацию незаконного вооруженного формирования, преступного сообщества (преступной организации), организованной группы для реализации массового убийства, а равно участие в такой структуре;

г) вербовку, вооружение, обучение и использование террористов (лиц, участвующих в террористической деятельности);

д) информационное или иное пособничество в планировании, подготовке или реализации массового убийства;

е) пропаганду идей массовых убийств, распространение материалов или информации, призывающих к осуществлению массовых убийств либо обосновывающих или оправдывающих необходимость осуществления такой деятельности.

Медийное сопровождение подготовки и осуществления актов скулшутинга, включая непосредственно сцены массовых убийств, производятся социальными сетями. Там же, через сетевые сообщества, желающие приобретают экипировку, постеры, фотообои и другие элементы субкультуры скулшутеров. Модерация сетевых сообществ скулшутеров осуществляется по той же схеме, что и боевиков-ингимаси[1]. Особенность нашей страны — низкая плотность населения при практически повсеместной доступности высокоскоростного интернета — делает скулшутинг идеальным инструментом для насыщающего террора в провинции, т.е. на большей части территории страны.

Основной массив актов скулшутинга, как предупрежденных, так и совершенных, приходится на малые города России: посе-

[1] Подробнее см.: *Сундиев И.Ю., Смирнов А.А., Андрюхин Н.Г.* Бесструктурные и бесконтактные способы вовлечения молодежи в террористическую и экстремистскую деятельность // Научный портал ВНИИ МВД России. 2018. № 2. С. 52–60.

ления от 1 тыс. человек до городов с населением 500 тыс. человек. Это суммарно в два раза больше, чем в «городах-миллионниках» (от 1 млн), включая Санкт-Петербург и Москву. Показательно, что во всех поселениях и малых городах, где произошли акты скулшутинга (от 1 тыс. до 50 тыс.), зафиксировано резкое сокращение населения на 30–50% от уровня 1990 г., они расположены на так называемых «депрессивных территориях».

Если в больших «миллионных» городах с высокой плотностью населения основным видом радикализма и терроризма являются уличные протестные акции и точечные террористические акты, то для разрушения «спокойной жизни» небольших поселений и городков (с критически низкой плотностью населения) наиболее чувствительным является именно скулшутинг.

Как показывает практика, в комплексной системе противодействия экстремистским и террористическим проявлениям в молодежной среде особо значимую роль играют ОРМ. Они направлены на выявление в цифросетевой среде сформировавшихся группировок и обеспечивающих их структур (торговцев атрибутикой, видеоконтентом и т.п.), осуществление документирования преступных действий в целях привлечения виновных к ответственности.

Основным способом получения информации о деятельности международных сетевых движений (в нашем случае — скулшутеров) выступает мониторинг цифросетевых ресурсов, мессенджеров и стриминговых каналов по маркерам-хештегам (таким как *Колумбайн*, *Естественный отбор*, *Natural selection*, *Wrath*, *Гнев*, *Ненависть*, *Убийцы*, *Эрик Харрис*, *Дилан Клиболд*, *Дилан Руф*, *Владислав Росляков*, *Columbine*).

Данную задачу на практике выполняют подразделения по борьбе с терроризмом ФСБ России (в 2020–2021 гг. ими предотвращены преступления, аналогичные казанскому, в Саратове, Красноярске, Волгограде, подмосковных Люберцах), а также подразделения по противодействию экстремизму и уголовного розыска (в части контроля за незаконным оборотом оружия и предотвращения убийств МВД России).

Другим важным инструментом противодействия деструктивным цифросетевым объединениям является мониторинг сетевой активности конкретных злоумышленников и вовлеченных ими лиц. Помимо классических методов ОРД для решения этих задач могут использоваться и новые технологии автоматизированного сбора и анализа информации в информационно-телекоммуникационных сетях по технологиям «больших данных». В этих целях необхо-

димо использование технических средств для обеспечения ОРМ — «СОРМ». Правовые основы применения СОРМ заложены в ст. 64 Федерального закона от 7 июля 2003 г. № 126-ФЗ «О связи», которая устанавливает обязанности операторов связи и ограничение прав пользователей услугами связи при проведении ОРМ, мероприятий по обеспечению безопасности Российской Федерации и осуществлении следственных действий.

Однако следует отметить и несколько иной тип систем мониторинга, в основе которых лежит проработка огромного массива разнообразных сведений из различных баз данных с целью получения определенных знаний (так называемые технологии ИИ, используемые при анализе данных). В правоохранительной деятельности таким искомым знанием чаще всего выступает ***информация, представляющая оперативный интерес***.

Благодаря использованию систем ИИ при анализе данных возможен автоматизированный мониторинг активности лиц, привлекающих несовершеннолетних к деструктивной деятельности через социальные сети, мессенджеры и стриминговые каналы, который, наряду с одновременным анализом информации о других типах их активности в офлайн-среде, способен помочь идентифицировать их и получить первичную информацию о замышляемых ими действиях, которые затем могут быть проверены и уточнены путем проведения ОРМ.

В целях их обнаружения и сбора информации требуется использовать конфидентов либо осуществлять легендированное внедрение и обеспечивать последующее участие сотрудников правоохранительных органов в закрытых сетевых сообществах, чатах и иных формах интернет-коммуникации преступников.

Для документирования преступной деятельности деструктивных цифросетевых сообществ в подразделениях по противодействию экстремизму должны применяться наработанные методики проведения ОРМ.

И.Ю. Сундиев, А.А. Смирнов

Оперативно-розыскная характеристика использования технологии геймификации в экстремистской и террористической деятельности

Игра — древнейший, «докультурный» уровень формирования знаний, умений и навыков, в том числе — межличностного взаимодействия. По мере развития человеческой культуры игры развивались, усложнялись, дифференцировались по социальным группам и целевому назначению[1].

Информационная революция и развитие ИКТ предопределили переход к созданию методов трансформации личности в заданном направлении — через внедрение игровых методик в различные области социальной деятельности. Например, в докладе «Будущее образования: глобальная повестка»[2], в разд. 3.4 «Тотальность игры» сказано: «*наиболее успешными являются игровые развивающие трансмедийные продукты длительного пользования, "взрослеющие" вместе с ребенком; в перспективе, именно "длинные" игры, существующие в виде шоу, дополненной реальности и других медиа, станут одним из основных форматов детского образования...*». Согласно представленной программе уже с начала 2020-х гг. виртуальные миры будут массово использоваться как «пространства передержки» и профессиональной переквалификации — как дешевая альтернатива системам переподготовки при центрах занятости.

Как и все новые социальные технологии, ***геймификация*** активно используется современными экстремистскими и террористическими организациями для бесконтактного и бесструктурного вовлечения игроков в преступные акции. Террористы занимаются вербовкой молодежи в чатах сетевых компьютерных игр, а также создают клоны игр с имитацией терактов. Об этом сообщил, выступая на открытии IX Московской конференции по международной безопасности 23 июня 2021 г., директор ФСБ России Александр

[1] Подробнее см.: *Хайзинга Й.* Homo Ludens. М., 1987.

[2] Будущее образования: глобальная повестка // Сколковский институт науки и технологий. URL: http://rusinfoguard.ru/wp-content/uploads/2016/12/GEF.Agenda_ru_full.pdf (дата обращения: 12.06.2021).

Бортников: «В особой группе риска молодежь, психологическая обработка которой ведется в социальных сетях и игровых чатах популярных многопользовательских компьютерных игр. Более того, исламистские группировки уже вышли на уровень создания собственных клонов таких игр, которые позволяют воздействовать на сознание потенциальных сторонников терроризма и экстремизма не только через голосовое общение, но и путем включения пользователя в игровые ситуации совершения терактов»[1].

1. Понятие, сущность и содержание геймификации как социальной технологии

Геймификация обычно определяется как «использование игровых методик в неигровых контекстах»[2]. Сам термин является транслитерацией англоязычного аналога «*gamification*» (он был предложен английским программистом Ником Пеллингом в 2002 г.).

Непосредственные причины активного использования геймификации во многом связаны с ростом индустрии компьютерных игр и активным увлечением ее продукцией молодежи. По мнению западных исследователей, компьютерные игры заменили музыку в качестве наиболее значимого компонента молодежной субкультуры[3]. Ресурс «Adweek» отмечал весной 2020 г., что доходы бизнеса компьютерных игр в США составляют 139 млрд долл. Эта сумма превышает совокупные доходы НХЛ, НБА, Национальной футбольной лиги и Главной лиги бейсбола США вместе взятых[4]. В 2020 г. мировая игровая индустрия заработала 180 млрд долл. — это на 20% больше, чем доходы от спорта и кино по всему миру[5].

---

1 Бортников заявил, что террористы создают клоны компьютерных игр с имитацией терактов // ТАСС. 2021. 23 июня. URL: https://tass.ru/obschestvo/11723253 (дата обращения: 23.06.2021).

2 *Deterding S., Dixon D., Khalad R. & Nacke L.* From game design elements to gamefulness: Defining 'gamification' // Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments (MindTrek '11). ACM, NewYork. NY, USA, 2011. P. 9–15.

3 *Monahan S.* Video games have replaced music as the most important aspect of youth culture // The Guardian. 11 Jan 2021. URL: https://www.theguardian.com/commentisfree/2021/jan/11/video-games-music-youth-culture?fbclid=IwAR0zH5C_eioD53G_aZcyIOBIA7hdvUOfa01558HitbZo5A5XToD6S_Vp9wg (дата обращения: 08.04.2021).

4 *Traeger P.* Gaming as a Cultural Force Just Stepped to the Forefront of Entertainment.

5 *Monahan S.* Video games have replaced music as the most important aspect of youth culture.

Процесс геймификации, связанный с применением игровых моделей в различных сферах деятельности, во многом обусловлен развитием не только самих компьютерных игр, но и иных компонентов цифровой среды: «удобство и распространение информационных технологий упростили процессы создания и внедрения элементов игры в социальное управление, снизили требования к необходимым организационным и материальным ресурсам для использования технологий геймификации, позволили эффектно оформлять игровые элементы»[1].

В. Меркурьев с соавторами выделяет ряд преимуществ технологии геймификации, связанных с психологическими особенностями личности[2].

1. *Использование потребности человека в целостных эмоциональных переживаниях* — применение игры позволяет обеспечить единство мыслей, чувств и действий, пробудить творческий потенциал, усилить ощущение солидарности и конкуренции.

2. *Принцип добровольности* — принцип игры предполагает добровольное участие или создание подобного ощущения у игроков.

3. *Вовлеченность участников в процесс* — геймификация усиливает вовлеченность участников в процесс, используя потребности в достижении успеха и поощрении, познании, общении, влиянии на других.

4. *Эксплуатация чувства безопасности* — игровая форма снимает напряжение участников и обеспечивает им ощущение защищенности, отсутствия угроз из-за нереальности происходящего в игре.

5. *Обеспечение эффекта «размытой ответственности»* — участие в игре снижает контроль и ответственность человека за свои поступки.

В качестве игровых элементов, применяемых при геймификации, выделяют: уровни (статусы), лидерборды (таблица лидеров/рейтингов), бейджи (виртуальные награды), очки и баллы, шкалу прогресса, продвижение по уровням, дайджесты успеха, интерактивные элементы, виртуальную валюту, виртуальные товары (продукция, которая продается за виртуальные деньги)[3].

---

[1] *Меркурьев В.В., Хлопкова О.В., Клементьев А.С.* Противодействие использованию технологий геймификации в террористических и экстремистских целях // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 89.

[2] Там же. С. 90.

[3] *Руднева Т.* Геймификация: что это такое, для чего нужно // Postium. 2019. 14 нояб. URL: https://postium.ru/gejmifikaciya-chto-eto-takoe/#:~:text=Геймификация%20-%20это%20когда%20элементы, и%20обменяй%20их%20на%20приз» (дата обращения: 09.04.2021).

Выделяют несколько игровых психотипов, проявляющихся в игре и обладающих определенным набором паттернов поведения: а) *накопитель* — игрок, для которого главной задачей является сбор всех бонусов и получение всех достижений; б) *киллер* — игрок, для которого главной задачей является победа над конкурентами и которым движут склонность к доминированию и жажда власти; в) *исследователь* — игрок, для которого важно изучить внутреннюю экосистему игры; г) *общительный* — игрок, для которого важен социальный контакт с другими пользователями или администрацией игры. Исходя из данной типологии можно подобрать игровую модель для взаимодействия с пользователями[1].

Следует отметить, что пандемия существенно усилила тенденцию роста востребованности компьютерных игр. По оценкам «Nielsen», среднее игровое время в 2020 г. выросло на 30–40%[2]. В социальном плане «широкое распространение и доступность игр и стриминговых сервисов превратили видеоигры в мощный инструмент влияния на аудиторию»[3].

2. Опыт и направления использования геймификации в террористической и экстремистской деятельности

Компьютерные игры как один из основных элементов массовой культуры были задействованы террористическими и экстремистскими организациями для достижения различных целей, включая вовлечение детей, донесение своих идей для широкой аудитории, усиление радикализации сторонников и интерактивное конструирование их идеальной реальности[4].

---

1 *Руднева Т.* Геймификация: что это такое, для чего нужно // Postium. 2019. 14 нояб. URL: https://postium.ru/gejmifikaciya-chto-eto-takoe/#:~:text=Геймификация%20—%20это%20когда%20элементы,и%20обменяй%20их%20на%20приз» (дата обращения: 09.04.2021).

2 *Корешкова Т.* Риски и угрозы, сопутствующие развитию индустрии киберспорта и гейминга // Научно-технический центр ФГУП «ГРЧЦ». 28.05.2021. URL: https://rdc.grfc.ru/2021/05/cybersport-and-gaming/ (дата обращения: 01.06.2021).

3 Там же.

4 *Schlegel L.* Ready Player One: How Video Games Could Facilitate Radicalization Processes // European Eye on Radicalization. 13 March 2020. URL: https://eeradicalization.com/ready-player-one-how-video-games-could-facilitate-radicalization-processes/ (дата обращения: 17.01.2021); *Сундиев И.Ю.* Информационные технологии в деятельности террористических и экстремистских организаций // Научный портал МВД России. 2011. № 4.

В киберпространстве с 1990-х гг. начался процесс стыковки технологий виртуальной реальности (ВР) с сетевыми технологиями. Первая такая реализация воплотилась в форме массовых многопользовательских сетевых ролевых игр (MMROPG). Получились настоящие обитаемые ВР-миры. ВР — это искусственный мир, генерируемый при помощи компьютеров, в который можно заходить, перемещаться, действовать и испытывать приключения. ВР может быть для индивидуального восприятия или для коллективного, как в MMROPG. В таких коллективных играх можно видеть других персонажей глазами своего персонажа, общаться с другими людьми через их персонажей и действовать с ними совместно.

Главная проблема — какой мир и какая реальность предлагаются в качестве поля взаимодействия. Компьютерная реальность может искажать у игрока историческую память (как, например, Blitzkrieg), может выключать эмпатию (Counter-Strike), может формировать установки на исключительно насильственные способы решения любых жизненных ситуаций. Сформировалась весьма своеобразная субкультура геймеров, часто теряющих границы между онлайном и офлайном[1].

В западной науке концепция геймификации была перенесена из сферы бизнеса в дискурс об экстремизме и радикализации преимущественно в связи с прямыми стримами нападений ультраправых террористов в Крайстчерче, Эль-Пасо и Галле. Хотя еще в 2011 г. американские консультанты по вопросам безопасности и внешней политики Дж. Брахман (J. Brachman) и А. Левин (A. Levine) отмечали использование принципов геймификации на сайтах джихадистской и праворадикальной направленности, стимулирующих активность их пользователей на основе конкуренции[2]. В последующие годы данный тренд получил дальнейшее развитие.

В настоящее время можно выделить несколько направлений и форм использования геймификации в террористической и экстремистской деятельности.

1. *Использование образов из компьютерных игр в пропагандистских материалах.* Принимая во внимание высокую популярность компьютерных игр, экстремисты активно используют содержа-

[1] Подробнее см.: *Степанцева О.* Субкультура геймеров в контексте информационного общества: дис. ... канд. культурологии. СПб., 2007.

[2] *Brachman J., Levine A.* The World of Holly Warcraft. How al Qaeda is using online game theory to recruit the masses // Foreign Policy. April 13, 2011. URL: https://foreignpolicy.com/2011/04/13/the-world-of-holy-warcraft (дата обращения: 19.03.2021).

щиеся в них персонажи, эстетику и сюжеты в своей пропагандистской деятельности. В частности, эксперты обращали внимание на присутствие образов и даже реальных сцен из популярного игрового шутера Call of Duty в пропагандистских роликах джихадистских группировок[1]. В 2017 г. телеграм-канал «Д///ихад» отметил появление кадров из онлайн-игры World of Warships в ролике ИГИЛ. Видеоряд с кораблями из игры возникает в самом начале экстремистского материала, который заканчивается казнью четырех пленников[2].

Ранее, в 2014 г., данная международная террористическая организация (МТО) выпустила видео, содержащее вырезанные и отредактированные минуты игрового сюжета Grand Theft Auto 5. Ролик был сделан с целью вербовки молодых людей, транслируя посыл о том, что террористы «делают то, что вы выполняете в играх, в реальной жизни на поле боя». В нем демонстрируются кадры игры с нападением на военный конвой и убийством полицейских[3].

Еще одним наглядным примером геймификации террористической пропаганды является демонстрация экрана с вариантами оружия для совершения террористических атак в пропагандистском ролике ИГИЛ «Побуждайте последователей» (*Incite the Believers*). Он выполнен по канонам компьютерных игр с указанием доступности оружия для игрока на текущем уровне. В ролике также сочетается нарезка кадров компьютерной графики и реальных видеозаписей, что, по мнению экспертов, размывает границы между насилием в игре и в реальной жизни[4].

Таким образом, использование образов популярных компьютерных игр выступает действенным приемом пропаганды экстре-

---

1 *Schlegel L.* Can You Hear Your Call of Duty? The Gamification of Radicalization and Extremist Violence // European Eye on Radicalization. 17 March 2020. URL: https://eeradicalization.com/can-you-hear-your-call-of-duty-the-gamification-of-radicalization-and-extremist-violence/ (дата обращения: 17.01.2021).

2 В ролике «Исламского государства» заметили кадры игры Worldof Warships // Лента.ру. 2017. 6 апр. URL: https://lenta.ru/news/2017/04/06/is_wow/ (дата обращения: 14.05.2021).

3 *Tassi P.* ISIS Uses 'GTA 5' In New Teen Recruitment Video // Forbes. Sep 20, 2014. URL: https://www.forbes.com/sites/insertcoin/2014/09/20/isis-uses-gta-5-in-new-teen-recruitment-video/?sh=6f57b47e681f (дата обращения: 20.05.2021).

4 *Wicks S.* Islamic State's Use of Gamification and Low-Tech Terror Tactics // Global Network on Extremism & Technology. 2 September 2020. URL: https://gnet-research.org/2020/09/02/iss-use-of-gamification-and-low-tech-terror-tactics/ (дата обращения: 27.05.2021).

мизма. Западные эксперты дискутируют на счет того, охватывает ли такая пропаганда лишь адептов и сторонников экстремистских организаций либо способна влиять и на более широкую аудиторию[1]. На наш взгляд, верен второй вариант ответа, и именно для этих целей радикалы задействуют символику наиболее рейтинговых и узнаваемых игр.

2. *Использование онлайн-стримов в террористической и экстремистской деятельности*. Помимо непосредственной игры в компьютерные игры, широкую популярность среди пользователей получили игровые ***стримы*** — видеотрансляции в сети прохождения игры определенным игроком или группой игроков. Наиболее востребованной платформой для игровых стримов является Twitch[2].

За последние годы было зафиксировано несколько случаев ведения *стримов* непосредственно в ходе реализации терактов, которые по своей стилистике очень напоминают игровые трансляции компьютерных шутеров от первого лица (*First-person Shooter*, *FPS*). Такой прием был использован в одном из наиболее резонансных терактов второго десятилетия XXI в., совершенном в г. Крайстчерче в Новой Зеландии. Его исполнитель Брентон Таррант заранее анонсировал свой теракт, а затем вел его прямую трансляцию на Facebook с помощью экшн-камеры. На видео нападавший комментировал ход атаки, как бы выступая перед аудиторией, и демонстрировал свое оружие, на котором были начертаны имена исторических личностей и сражения в борьбе европейских держав против Османской империи. Атака транслировалась в прямом эфире в течение 17 минут и просматривалась не менее 4 тыс. раз, прежде чем Facebook отключил ссылку. В течение следующих 24 часов Facebook удалил еще 1,5 млн копий видео атаки со своих страниц.

Из-за широкого резонанса теракта, сделавшего из Тарранта «икону» для мирового ультраправого движения, тактика применения *стримов*, несомненно, получит дальнейшее распространение в качестве мощного инструмента привлечения общественного внимания. Показательно, что вдохновленный новозеландским терактом мужчина, совершивший нападение на синагогу в американском г. Пауэе 27 апреля 2019 г., также планировал вести его онлайн-

[1] *Robinson N., Whittaker J.* Playing for hate // Global Network on Extremism & Technology. 1 March 2021. https://gnet-research.org/2021/03/01/playing-for-hate/ (дата обращения: 27.05.2021).

[2] *Брызгалова Е.* Каждый третий пользователь рунета смотрит стримы, а каждый восьмой стримит сам // Ведомости. 2019. 2 авг. URL: https://www.vedomosti.ru/technology/articles/2019/08/01/807883-kazhdii-smotrit-strimi (дата обращения: 03.03.2021).

трансляцию в Facebook[1], а исполнитель теракта в немецком Галле такую трансляцию вел через игровую онлайн-платформу Twitch[2].

Вполне возможно распространение подобных политических заявлений посредством онлайн-стримов координаторами и участниками незаконных протестных акций, проповедниками экстремистских движений. В то же время использование прямых трансляций лидерами крупных международных террористических организаций представляется маловероятным из-за вероятности раскрытия ими своего местоположения.

3. *Встраивание игровых элементов в пропагандистские материалы и коммуникационные приложения.* Данное направление наиболее четко выражает общепризнанное понимание геймификации и объединяет различные формы встраивания игровых элементов и методик в информационную активность экстремистов.

Дж. Брахман и А. Левин, одними из первых обратившие внимание на внедрение геймификации в деятельность радикалов, в качестве используемых ими игровых элементов выделили присвоение баллов, определенных рейтингов и статусов. В качестве примера они приводят британский исламистский экстремистский сайт «Salafi Media», который измерял уровень вовлеченности пользователей «метром фундаментализма». Чем более «радикальным» или «фундаменталистским» становился пользователь, тем больше власти и легитимности он приобретал на форуме. Следствием применения таких игровых методик выступает увеличение числа посетителей экстремистских ресурсов и проводимого на них времени. Однако применение принципов геймификации не ограничивается интернетом: журнал ИГИЛ «Inspire» публиковал игровые задания для своих читателей, такие как «сделать бомбу на кухне вашей мамы» и «осуществить Мумбаи [атаку] возле Белого дома, чтобы стать мучеником»[3].

Как отмечают российские эксперты, «при помощи технологий геймификации организаторы террористической деятельности

---

1 *McGowan M.* San Diego shooting suspect posted 'open letter' online // The Guardian, 28 April 2019. URL: https://www.theguardian.com/us-news/2019/apr/28/john-earnest-san-diego-shooting-suspect-postedopen-letter-online (дата обращения: 17.01.2021).

2 *Koehler D.* The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat // CTC Sentinel. 2019. Vol. 12. Is. 11. Dec. P. 14–20.

3 *Brachman J., Levine A.* The World of Holly Warcraft. How al Qaeda is using online game theory to recruit the masses // Foreign Policy. 13 April 2011. URL: https://foreignpolicy.com/2011/04/13/the-world-of-holy-warcraft (дата обращения: 19.03.2021).

могут ранжировать потенциальных и реальных участников экстремистских ячеек, выявлять наиболее активных и эффективных игроков. Эти люди с большой вероятностью могут быть назначены лидерами ячеек, групп либо исполнителями наиболее важных и сложных поручений»[1].

Одним из достаточно свежих примеров применения игровых методик для вовлечения в экстремистскую активность выступает приложение PatriotPeer («Радар патриота»), самостоятельно разработанное идентитаристским движением (Identitarian Movement) и представленное лидером его австрийского подразделения Мартином Зельнером. Patriot Peer представляет собой социальный сервис, сочетающий возможности Tinder и Pokemon Go и позволяющий членам движения обнаруживать друг друга поблизости на карте и встречаться для общения. Сервис имеет элементы геймификации, присваивая и накапливая баллы для наиболее активных его участников[2].

Еще один пример «само-геймификации» описан К. Макдональдом. Британские подростки создали виртуальную группу в WhatsApp, чтобы бороться с «колдунами», под которыми понимались религиозные лидеры мусульманских групп, воспринимаемые как отступники. Участники группы совершали «рейды», вламываясь в дома «колдунов», чтобы украсть предметы «черной магии», а затем делились своим опытом в сети. Такой сценарий действий очень напоминает набеги на темницы и обмен пройденными «квестами» между участниками известных многопользовательских игр, таких как World of Warcraft. В этом случае границы между играми и реальностью размываются. Воображаемые персонажи и их роль как «игрового клана» с миссией в игровой сфере были перенесены в офлайн-мир[3].

4. *Создание компьютерных игр, сценарий которых связан с осуществлением экстремистской деятельности.* Данное направление геймификации включает компьютерные игры, сценарий которых

---

1 *Меркурьев В.В., Хлопкова О.В., Клементьев А.С.* Противодействие использованию технологий геймификации в террористических и экстремистских целях // Всероссийский криминологический журнал. 2020. Т. 14. № 1. С. 91.

2 *Prinz M.* „PATRIOT PEER“ ALS MISCHUNG AUS TINDER UND POKEMON GO // BellTower news. 28 Feb 2017. URL: https://www.belltower.news/heimatliebe-im-app-store-patriot-peer-als-mischung-aus-tinder-und-pokemon-go-43312/ (дата обращения: 25.01.2021).

3 *McDonald K.* Radicalization. Citation by: *Schlegel L.* Points, Rankings & Raiding the Sorcerer's Dungeon...

предполагает осуществление насильственных и иных экстремистских действий и в виртуальной, и в офлайн-среде.

Одним из первых таких примеров стала игра «Этническая чистка», персонажи которой в образе членов Ку-клукс-клана или скинхедов охотились на «агрессивных человекоподобных существ» и «их еврейских хозяев» на улицах европейских городов. Национальный директор европейской Антидиффамационной лиги Авраам Фоксман, комментируя выход игры, в 2002 г. заявил, что «расисты находят способы использовать современные технологии для распространения в массовой аудитории идей белого супрематизма, антисемитизма и ненависти»[1].

Кроме того, в статье Е. Журавлевой описана модифицированная версия известного шутера «Побег из замка Волфенштейн», в которой главные герои этой игры занимались отстрелом негров. Зарубежные эксперты приводят и другие примеры компьютерных игр экстремистского характера, включая игры белого супрематизма (White Law (2003), ZOG's Nightmare (2006)[2], ZOG's Nightmare II (2007) и игры исламистских групп (Hezbollah's Special Force))[3].

Существует также пласт компьютерных игр, сюжет которых завязан на сценарии проведения протестных акций и организации революций. Примером такой игры является 3D-стратегия *Republic*: *The Revolution*, разработанная компанией «Elixir Studios». События игры происходят в вымышленной Новострании — бывшей советской республике, ставшей самостоятельным государством после распада СССР. Игровой сценарий предполагает борьбу одной из множества оппозиционных партий против коррумпированного диктатора Карасева, недовольство которым в народе растет. Игровой персонаж в начале сюжета возвращается в город Екатеринск и вступает в борьбу за политическую власть. Для этого он создает партию, начинает ее раскрутку с целью завоевания популярности населения и борьбу с конкурентами. В дальнейшем он начинает реализовывать идею создания подпольной сети и организации революции для свержения диктатора.

---

1 *Журавлева Е.* Грязные игры: Кто и почему втягивает геймеров в политическую борьбу // Популярная механика. 30.05.2006. URL: https://www.popmech.ru/technologies/5476-gryaznye-igry-kto-i-pochemu-vtyagivaet-geymerov-v-politicheskuyu-borbu/ (дата обращения: 21.05.2021).

2 Аббревиатура ZOG в лексиконе правых экстремистов означает «сионистское оккупационное правительство» (Zionist Occupation Government).

3 *Robinson N., Whittaker J.* Playing for hate // Global Network on Extremism & Technology. 1 March 2021. URL: https://gnet-research.org/2021/03/01/playing-for-hate/ (дата обращения: 27.05.2021).

Набор игровых опций достаточно широк, вот как он описан в рецензии: «А в The Revolution игроку предлагалось пройти путь от основателя партийной ячейки до президента государства — и при этом вовсе не стесняться в средствах, применяя политические, финансовые, преступные, религиозные и военные методы... Игроку предлагалось вести опасную политическую игру, совмещая подкупы видных общественников и заказные убийства конкурентов с храбрыми речами и активной партработой. Хотите быть олигархом? Пожалуйста! Основать преступный синдикат? Сколько угодно! Организовать "бархатную революцию" или провести путч? Да запросто!»[1]. Выручка от продажи игры не окупила вложенных затрат, но через год в одной из постсоветских стран действительно произошли аналогичные сюжету игры события, и игровая оранжевая эмблема превратилась в оранжевые банты и флажки[2].

Еще более наглядным примером компьютерной игры, используемой для обучения тактике протестных действий, является пошаговая стратегия *A Force More Powerful* (*AFMP*), выпущенная в 2006 г. Игра разработана Международным центром ненасильственного конфликта (*International Center on Nonviolent Conflict*, *ICNC*) в сотрудничестве с компанией «Break Away Games». Она завершила линейку информационных продуктов с таким названием, первым из которых стал документальный фильм (1999 г.), а вторым — книга (2001 г.). При выходе игры было заявлено, что AFMP — это «первая и единственная игра, обучающая методам влияния или изменения политической обстановки ненасильственными способами. Она предназначена для использования активистами и лидерами сопротивления и движений оппозиции»[3]. Игра содержит «дюжину сценариев, основанных на реальных событиях, включая выступления против диктаторов, оккупантов, колонизаторов и коррумпированных режимов, показывает борьбу за права человека, этнических и расовых меньшинств и женщин», а пользователей обучают «стратегическому планированию, формулировке целей (типа требования свободных выборов или отставки дикта-

[1] *Хорев Т.* Republic: TheRevolution (Республика: Революция) // Игромания. 17.03.2004. URL: https://www.igromania.ru/article/3473/Republic_The_Revolution_(Respublika_Revolyuciya).html (дата обращения: 24.05.2021).

[2] *Сундиев И.Ю., Смирнов А.А.* Теория и технологии социальной деструкции в XXI веке (на примере «цветных революций»). М.: Русский биографический институт, Институт экономических стратегий, 2016. С. 239.

[3] *Болотов К.* Игра готовит оппозицию к борьбе с диктатурой и кровавым режимом // MEMBRANA. 27.10.2005. URL: http://www.membrana.ru/particle/476 (дата обращения: 27.04.2013).

тора), выбору тактики (например, забастовок, акций протеста или бойкотов)»[1].

Игре дал высокую оценку один из основателей сербской группы студенческого сопротивления «Отпор» Иван Маровић: «*...игра поможет оппозиции больше, чем кино или литература, поскольку активисты смогут моделировать различные ситуации и опробовать различные стратегии прежде, чем испытать их в действии*»[2].

В 2019 г. вышла подобная игра — «симулятор восстаний» — под названием *RIOT — Civil Untrest*. Ее создатель Леонард Менчиари также имеет реальный опыт участия в протестах в Италии и создавал игру, чтобы поделиться своим опытом. Симулятор дает возможность играть за обе стороны конфликта. Для протестующих предусмотрен широкий набор игровых действий, начиная от ненасильственных и заканчивая атаками на полицию с коктейлями Молотова[3].

Наиболее опасной формой геймификации экстремизма выступает применение «*игр в альтернативной реальности*» (*alternate reality game, ARG*) — интерактивных игр, в которых игровой платформой выступает реальный мир. Авторы таких игр создают целостный игровой мир со своими героями, сюжетом и атмосферой[4]. Залогом успеха игр с альтернативной реальностью выступает их правдоподобность, стирание грани между игрой и действительностью.

Известным примером применения ARG являлся российский интернет-проект «Большая игра. Сломай систему»[5]. Проект был

---

1 *Болотов К.* Игра готовит оппозицию к борьбе с диктатурой и кровавым режимом // MEMBRANA. 27.10.2005. URL: http://www.membrana.ru/particle/476 (дата обращения: 27.04.2013).

2 *Журавлева Е.* Грязные игры: Кто и почему втягивает геймеров в политическую борьбу // Популярная механика. 30.05.2006. URL: https://www.popmech.ru/technologies/5476-gryaznye-igry-kto-i-pochemu-vtyagivaet-geymerov-v-politicheskuyu-borbu/ (дата обращения: 21.05.2021).

3 *Коршунов С.* На баррикады! Игры про революцию и борьбу с режимом // УНИАН игры. 2020. 6 июня. URL: https://www.unian.net/games/top-5-igr-pro-revolyuciyu-i-borbu-s-rezhimom-igry-11026028.html (дата обращения: 24.05.2020).

4 *Persianinov R.* Всё, что нужно знать об играх в альтернативной реальности // TJ. 2017. 4 июля. URL: https://tjournal.ru/flood/45950-arg (дата обращения: 04.04.2021).

5 *Сундиев И.Ю.* Информационные технологии в экстремистской деятельности молодежных объединений // Научный портал МВД России. 2010. № 2. С. 19–21; *Горев А.И.* Информационные методы противодействия экстремизму и терроризму // Научный портал МВД России. 2010. № 3. С. 112–123.

запущен националистическим движением «Северное братство»[1] в 2007 г. и может считаться одним из первых и наиболее «продвинутых» образцов геймификации экстремизма. Это отчасти объясняется тем, что в числе его разработчиков выступал бывший сотрудник Института системного анализа Российской академии наук, доктор технических наук Петр Хомяков, впоследствии осужденный за экстремизм. Смысл самой «Игры» заключался в осуществлении акций, направленных как на пропаганду идей «Северного братства», так и на психологический и физический террор в отношении работников «Системы» (сотрудников правоохранительных органов) и «пришельцев» (мигрантов и лиц неславянской национальности)[2].

В «Большой игре» участвовали команды единомышленников (по терминологии игры, «автономные группировки»), которые регулярно получали на свои e-mail списки заданий различного уровня сложности. Например, от игроков требовалось бить витрины, поджигать двери и забрасывать петардами принадлежащие неславянам кафе и магазины, переворачивать и жечь машины, рисовать свастики и нацистские лозунги на стенах домов, избивать и казнить «пришельцев». Игрокам также предстояло подбрасывать под окна приемных «Единой России», избиркомов (на сленге игроков, «лохотронов») или опорных пунктов милиции фальшивые «бомбы». Игроки должны были выискивать контактные данные (домашние адреса, телефоны) местных чиновников, бизнесменов, силовиков и правозащитников и отправлять их на e-mail организаторов.

Выполнение каждого задания должно было подтверждаться фото- или видеозаписью, которая отправлялась на сайт «Большой игры», за что игрок получал баллы. Таким образом происходил формальный переход от онлайна к офлайну. Авторы игры признавались, что их цель — «создать сеть автономных группировок, ненавидящих Систему и постепенно увеличивающих свои умения и навыки для их последующего применения уже в прямых столкновениях с Системой». В архиве сайта «Большой игры» насчитывалось несколько десятков тысяч видеосюжетов о выполненных «заданиях», т.е. о совершенных преступлениях экстремистской направленности[3]. Одним из доказанных эпизодов криминальной дея-

[1] В 2012 г. движение признано экстремистской организацией, и его деятельность в России запрещена.

[2] Северное братство // Антикомпромат. URL: http://www.anticompromat.org/nazi-p/sev_br.html (дата обращения: 12.02.2018).

[3] *Сундиев И.Ю., Смирнов А.А.* Теория и технологии социальной деструкции в XXI веке (на примере «цветных революций»). М.: Русский биографический институт, Институт экономических стратегий, 2016. С. 243–244.

тельности участников «Большой игры» является случай в г. Невинномысске Ставропольского края, где студент И. Карцев, участвуя в интернет-проекте, подложил муляж взрывного устройства к зданию отдела УФСБ, а впоследствии обстрелял из охотничьего ружья жителей города, за что был приговорен Невинномысским городским судом к полутора годам лишения свободы[1]. В последующем проект «Большая игра» был признан экстремистским, а его основатель А. Мухачёв осужден за организацию экстремистского сообщества[2].

Позже данная игровая модель получила свое применение и в механизме подстрекательства несовершеннолетних к совершению суицида в так называемых группах смерти — суицидальных виртуальных сообществах, созданных в социальных сетях. В них подростки выполняли задания, которые им последовательно давались «кураторами» суицидальных пабликов (сама «игра» получила сленговое название «синий кит» из-за активного использования образа данного млекопитающего). Задания предусматривали нанесение ребенком себе порезов на руки, ночное пробуждение и просмотр определенного контента, выполнение «квестов» (сделать селфи на крыше высотного дома, пробежать перед машиной и т.п.). Заключительным заданием выступало совершение самоубийства. Кейс «синих китов» также выделяется созданием антуража таинственности и использованием мифологических конструкций популярных молодежных субкультур, в частности образа «тихого дома» субкультуры нетсталкеров, в игровом сюжетном сценарии[3].

---

1 *Ларинцева А.* «Большая игра» завела в колонию // Коммерсантъ. 2009. 28 янв. URL: http://www.kommersant.ru/doc/1109376 (дата обращения: 03.03.2018).

2 Интернет-проект «Большая игра «Сломай систему» признан экстремистским // ИА REGNUM. 02.03.2010. URL: http://www.regnum.ru/news/1258963. html?forprint (дата обращения: 03.03.2018); Создатель интернет-проекта «Большая Игра. Сломай Систему» за планы «бархатной» революции в РФ осужден на 9 лет // Право.ru. 2011. 30 сент. URL: http://pravo.ru/news/view/61736/ (дата обращения: 03.03.2018).

3 *Сундиев И.Ю., Смирнов А.А., Курицын А.Н.* Теория и технологии социальной деструкции в XXI веке (на примере «цветных революций») // Проблемы социальных конфликтов в современной психологии: сущность, детерминанты, регулирование. М.: Изд-во Института психологии РАН, 2018. С. 334–342.

3. Противодействие использованию технологий геймификации в террористической и экстремистской деятельности

Ниже будут представлены некоторые предложения по противодействию применению технологий *геймификации*, используемых для террористической и экстремистской деятельности. Однако сразу отметим, что геймификация не является какой-либо самостоятельной формой проявлений терроризма и экстремизма. Напротив, теоретический конструкт геймификации описывает лишь варианты встраивания игровых методик и сюжетов в «классические» направления экстремистской деятельности, такие как пропаганда, вербовка и радикализация.

И потому главным «рецептом» борьбы с технологиями геймификации терроризма и радикализма будет принятие их во внимание при выработке соответствующих мер противодействия. Вместе с тем может потребоваться принятие комплекса специальных мер в рамках следующих направлений.

1. *Регулирование оборота информационной продукции*. Меры в рамках этого направления могут потребоваться для ограничения распространения на территории страны компьютерных игр, сценарий которых связан с осуществлением экстремистской деятельности. В соответствии с национальным законодательством могут быть введены запрет на оборот таких игр либо возрастные ограничения в рамках механизма возрастной классификации и маркировки информационной продукции (в России такой механизм установлен Федеральным законом от 29 декабря 2010 г. № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию»).

2. *Ограничение доступа к информации в сети Интернет*. Для ограничения доступа к материалам игрового характера (начиная от самих компьютерных игр и заканчивая публикациями игровых заданий в сети Интернет) могут применяться действующие организационно-правовые механизмы блокировки. В случае если речь идет о размещении контента в социальных сетях и мессенджерах, требуется организация взаимодействия с администрациями данных платформ в целях удаления такого контента, выявления его распространителей и блокировки их аккаунтов.

3. *Криминализация отдельных форм геймификации экстремистской деятельности* предполагает установление уголовной и (или) административной ответственности за отдельные правонарушения, связанные с задействованием игровых методик. Например,

в России для борьбы с деятельностью так называемых «кураторов» суицидальных сообществ («групп смерти») потребовалось введение в УК РФ двух новых составов преступлений, так как имевшаяся ст. 110 «Доведение до самоубийства» не во всех случаях позволяла привлечь к ответственности лиц, склонявших детей к самоубийству через игровые методики. Поэтому новой ст. 110.1 УК РФ было криминализировано склонение к совершению самоубийства путем уговоров, предложений, подкупа, обмана или иным способом при отсутствии признаков доведения до самоубийства, а также содействие совершению самоубийства советами, указаниями, предоставлением информации, средств или орудий совершения самоубийства либо устранением препятствий к его совершению или обещанием скрыть средства или орудия совершения самоубийства. Для тех лиц, которые сами не склоняли детей, но создавали информационные ресурсы с суицидальным контентом для привлечения внимания несовершеннолетних ст. 110.2 УК РФ была установлена ответственность за организацию деятельности, направленной на побуждение к совершению самоубийства путем распространения информации о способах совершения самоубийства или призывов к совершению самоубийства.

Указанные статьи предоставили правоохранительным органам возможность применить обычные инструменты оперативно-розыскной и уголовно-процессуальной деятельности для пресечения деятельности виртуальных суицидальных сообществ. И благодаря этому силовым структурам России данную угрозу удалось успешно нейтрализовать.

4. *Информационно-разъяснительная и контрпропагандистская работа*. Сведения об опасности и о возможных формах использования геймификации в террористической и экстремистской деятельности должны быть включены в имеющиеся и перспективные программы профилактической работы в рассматриваемой сфере. Некоторые проявления геймификации могут потребовать и контрпропагандистских усилий, направленных на разоблачение истинных целей организаторов опасных игр, снижение их популярности у молодежи и предложение позитивных альтернатив.

Для данного направления следует сделать одну оговорку. Кейс «синих китов» в России показывает, что иногда широкое освещение в СМИ и социальных сетях определенных угроз само по себе служит фактором их разрастания. Поскольку оно привлекает внимание широких слоев населения, вызывает «моральную панику» и, самое главное, стимулирует интерес к теме детей. В случае «групп

смерти» последнее обстоятельство не только привело к всплеску интереса молодежи к данной теме, но и породило возникновение так называемых «псевдокураторов» — подростков, которые, не будучи вовлеченными в организованные сетки суициальных сообществ, по своей инициативе решали попробовать довести кого-то до самоубийства из «спортивного интереса». К сожалению, у части из них это получилось. Поэтому информационная работа с целью повышения осведомленности о деструктивных технологиях геймификации должна проводиться аккуратно, чтобы, с одной стороны, проинформировать родителей, педагогов и иных ответственных лиц, а с другой — не «подогреть» интерес к теме у несовершеннолетних.

* * *

Как было показано, технологии геймификации задействуются террористами и экстремистами для пропаганды, вербовки и вовлечения в противоправную деятельность.

Пока наблюдается спорадическое задействование таких технологий в деятельности различных джихадистских, праворадикальных и иных организаций. Однако в глобальном информационном пространстве любая эффективная практика радикализации получает широкое распространение. Это отчетливо проявилось в случае теракта в Новой Зеландии, транслировавшегося в режиме реального времени в сети и спровоцировавшего волну схожих атак в разных странах мира с попытками прямых стримов.

Наибольшую опасность среди технологий геймификации представляет создание экстремистских игр в альтернативной реальности, предполагающих выполнение игровых заданий (терактов и иных экстремистских акций) в реальном мире. Это один из наиболее перспективных способов бесструктурного способа вовлечения в противоправную деятельность.

В связи с этим можно прогнозировать, что геймификация станет неотъемлемым элементом информационных стратегий террористических и экстремистских организаций. Этот вызов требует выработки адекватных механизмов нейтрализации его проявлений. Ответ должен быть комплексным и включать в себя систему точечных мер мониторинга и противодействия данной угрозе, в том числе меры по ограничению оборота информационной продукции, блокировке определенного контента и ресурсов, криминализации наиболее опасных форм геймификации, ведению информационно-разъяснительной и контрпропагандистской работы.

Вместе с тем технологии геймификации следует воспринимать и как возможность, которая открывается для оперативных подразделений субъектов ОРД в плане потенциального пополнения собственного арсенала традиционных средств борьбы с угрозами, включая терроризм и экстремизм, новыми инструментами и методиками работы.

М.А. Кочубей, А.А. Смирнов

Цифровой экстремизм и его значение для оперативно-розыскной деятельности

Для ОРД оперативных подразделений органов МВД России и ФСБ России важно учитывать цифровой потенциал, который задействуется террористическими и экстремистскими структурами. В основных документах стратегического планирования в области национальной безопасности — в Стратегии национальной безопасности Российской Федерации[1], Стратегии противодействия экстремизму в Российской Федерации до 2025 года[2], Доктрине информационной безопасности Российской Федерации[3] и др. — идентифицируется в качестве угроз деятельность, связанная с использованием ИКТ для распространения и пропаганды идеологии терроризма и экстремизма, вовлечения в террористическую и экстремистскую активность, организации и координации противоправных акций. Так, в Доктрине информационной безопасности РФ отмечается, что террористические и экстремистские группировки используют возможности современных ИКТ для ведения пропагандистской и вербовочной деятельности, «информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников».

Данные угрозы зафиксированы и на международном уровне — в Глобальной контртеррористической стратегии ООН, принятой резолюцией A/RES/60/288 Генеральной Ассамблеи от 8 сентября

---

1 Стратегия национальной безопасности Российской Федерации: утв. Указом Президента РФ от 2 июля 2021 г. № 400 // СЗ РФ. 2021. № 21 (ч. 2). Ст. 5351.

2 Стратегия противодействия экстремизму в Российской Федерации до 2025 года: утв. Указом Президента РФ от 29 мая 2020 г. № 344 // Официальный интернет-портал правовой информации. 25.05.2020. URL: http://publication.pravo.gov.ru/Document/View/0001202005290036?index=0&rangeSize=1 (дата обращения: 21.03.2021).

3 Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 декабря 2016 г. № 646 // СЗ РФ. 2016. № 50. Ст. 7074.

2006 г.[1], Соглашении между правительствами государств — членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г.[2], Конвенции Совета Европы о предупреждении терроризма от 16 мая 2005 г.[3], Договоре о сотрудничестве государств — участников СНГ в борьбе с терроризмом от 4 июня 1999 г.[4], Шанхайской Конвенции о борьбе с терроризмом, сепаратизмом и экстремизмом (г. Шанхай, 15 июня 2001 г.)[5], Конвенции ШОС по противодействию экстремизму от 9 июня 2017 г.[6] и других подобных документах.

Международными организациями, компетентными органами национальных государств и экспертным сообществом проводится большой объем аналитической работы по изучению проявлений терроризма и экстремизма в цифровой среде. В настоящем материале будут изложены некоторые значимые результаты такого анализа.

Основные направления использования цифровой среды в террористических и экстремистских целях

Террористическими и экстремистскими акторами возможности ИКТ применяются для реализации различных форм своей противоправной активности. Наиболее изученными в этом плане являются интернет-технологии. Видный израильский эксперт *Г. Вейман* выделил восемь способов использования интернета террористами: 1) ведение психологической войны; 2) поиск информации; 3) обучение; 4) сбор денежных средств; 5) пропаганда; 6) вербовка; 7) организация сетей; 8) планирование и координация террористических действий[7]. Схожий перечень приводится в специальном аналитическом докладе Управления ООН по наркотикам и преступности

---

1 Организация Объединенных Наций. URL: https://undocs.org/ru/A/RES/60/288 (дата обращения: 03.04.2021).

2 Бюллетень международных договоров. 2012. № 2.

3 Бюллетень международных договоров. 2009. № 9.

4 Бюллетень международных договоров. 2006. № 9.

5 Бюллетень международных договоров. 2004. № 1.

6 Официальный интернет-портал правовой информации. URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=102574570&backlink=1&&nd=102632751 (дата обращения: 14.02.2021).

7 *Вейман Г.* Как современные террористы используют Интернет. Специальный доклад № 116 // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/analytics/Tropina_01/ (дата обращения: 12.04.2013).

(UNODC) «Использование Интернета в террористических целях»[1] (далее — Доклад ЮНОДК): 1) пропаганда (в том числе вербовка, радикализация и подстрекательство к терроризму), 2) финансирование; 3) подготовка террористов; 4) планирование (в том числе с использованием секретной связи и открытых источников информации); 5) исполнение; 6) кибератаки.

Кратко рассмотрим основные направления использования интернета в деятельности террористических и экстремистских организаций на основе анализа названных источников.

Пропаганда оценивается как приоритетное направление использования интернета террористами. Основные цели состоят в максимально широком распространении своих идей среди населения и оказании психологического воздействия на целевые группы (сторонников, реальных или потенциальных жертв, правительство, международное сообщество).

Обычно пропагандистские материалы имеют форму мультимедийных коммуникаций, содержащих идеологические или практические наставления, разъяснения, оправдания или рекламу террористической деятельности. К ним могут относиться виртуальные сообщения, презентации, журналы, теоретические работы, аудио- и видеофайлы, а также электронные игры, разрабатываемые террористическими организациями или их сторонниками. Основными источниками пропаганды в сети Интернет являются разнообразные интернет-порталы (официальные и неофициальные СМИ, сайты организаций и др.), интернет-форумы различной направленности, блоги, социальные сети и видеохостинги.

Широкая область влияния распространяемой через интернет информации значительно увеличивает аудиторию, на которую она может воздействовать. При этом, как отмечается в исследовании группы зарубежных авторов, «радикальные группы разрабатывают способы усиления идеологической приверженности посредством (1) ограничения доступа к информации или обстоятельствам, которые бросают вызов идеологическим конструктам, и (2) социальных и когнитивных стратегий усиления внутригрупповых предубеждений и ненависти к людям вне группы. Экстремистские группы создают самоподкрепляющуюся социальную среду»[2].

---

[1] Использование Интернета в террористических целях (Управление Организации Объединенных Наций по наркотикам и преступности, 2013).

[2] *Brown R.A., Helmus T.C., Ramchand R., Palimaru A.I., Weilant S., Rhoades A.L., Hiatt L.* Violent Extremism in America // RAND, 2021. URL: https://www.rand.org/pubs/research_reports/RRA1071-1 (дата обращения: 02.05.2021).

Для обеспечения большей доступности террористические группы создают многоязычные сайты. Простой порядок размещения контента в интернете устраняет зависимость террористических организаций от СМИ, редакционная политика которых может блокировать распространение пропагандистской информации о террористах.

Вербовка и подстрекательство. Интернет-ресурсы активно используются в деятельности экстремистских и террористических организаций для привлечения новых участников. Совокупная аудитория интернета обеспечивает данным организациям глобальный резерв потенциальных новобранцев. Для целей вербовки могут использоваться как информационные сайты террористов, так и коммуникационные веб-платформы: чаты, блоги, социальные сети, IP-телефония и мессенджеры, электронная почта. Еще одним средством вовлечения сторонников (особенно несовершеннолетних) в террористическую деятельность служат онлайновые компьютерные игры, которые могут предусматривать выполнение «заданий» не только в виртуальном пространстве, но и в реальной жизни (совершение актов насилия, погромов, иных действий по устрашению).

Подстрекательство состоит в распространении информации и ведении коммуникаций, направленных на склонение конкретного либо неперсонифицированного лица или группы к совершению терактов и экстремистских преступлений. Как правило, оно предполагает индивидуальное общение в социальных сетях и мессенджерах с потенциальным исполнителем с целью склонения его к реализации задуманного. Как правило, для этого используются «приватные» инструменты коммуникации, такие как закрытые чаты, электронная почта и IP-телефония.

В Докладе ЮНОДК отмечается, что грань между пропагандой терроризма и подстрекательством к совершению терактов зачастую достаточно тонкая. Промежуточной ступенью между первичной вербовкой и непосредственно подстрекательством к совершению теракта является психологическая обработка неофита с целью привития ему экстремистских взглядов и обеспечения готовности к активным действиям (радикализация).

Подготовка (обучение) террористов. Интернет обеспечивает возможность широкого распространения учебно-методической литературы и мультимедийных обучающих материалов, касающихся тактики подготовки и совершения терактов, самодельного изготовления оружия и взрывных устройств, сбора необходимой информации, обеспечения защиты используемых каналов коммуникации

и т.п. Существуют даже виртуальные учебные лагеря, предоставляющие инструкции по использованию оружия в форме дистанционного электронного обучения[1]. Еще одной формой обучения террористов являются онлайн-инструктажи, проводимые в режиме реального времени посредством электронных средств коммуникации.

Планирование и координация деятельности. Данное направление включает в себя несколько составляющих. Одной из них является использование интернета для сбора информации из открытых источников о потенциальных объектах террористической атаки, возможных орудиях и средствах ее совершения. Могут применяться популярные интернет-сервисы, в частности геоинформационные ресурсы (например, GoogleEarth) и социальные сети (например, Facebook).

Другим аспектом является использование интернета в качестве канала коммуникации (связи) между различными ячейками террористической организации или отдельными ее членами как в «повседневной» деятельности, так и при планировании и осуществлении конкретного теракта. Для этих целей задействуются интернет-мессенджеры, электронная почта, IP-телефония.

Финансирование. Террористические и экстремистские организации используют возможности интернета для финансового обеспечения своей деятельности. Оно включает в себя несколько направлений сбора средств:

а) сбор пожертвований — осуществляется путем прямых призывов о пожертвовании средств, размещаемых на веб-сайтах, в чатах или социальных сетях и распространяемых посредством массовых рассылок;

б) электронная торговля — включает организацию интернет-магазинов, предлагающих информационные материалы (книги, аудио- и видеозаписи), символику и атрибутику и т.д.;

в) использование платежных систем в интернете — предполагает применение данных систем для электронного перевода средств террористическим организациям, а также совершение актов интернет-мошенничества с помощью таких приемов, как хищение личных данных, кража кредитных карт и т.д.;

г) посредничество благотворительных организаций — включает создание фиктивных «благотворительных» организаций для сбора средств или внедрение в существующие организации для оказания поддержки террористическим формированиям.

---

[1] Понимание киберпреступности: явление, задачи и законодательный ответ (подгот. М. Герке, Международный союз электросвязи, 2012). С. 37.

В последние годы спецслужбы фиксируют активное использование экстремистами криптовалют.

В период пандемии в механизмах финансирования террористической и экстремистской деятельности произошли изменения. Во многом этому способствовал уход больших сегментов экономики и финансовой активности граждан в онлайн. Сектор теневых веб-рынков существенно расширился. Множатся серии фишинговых атак, стремительно растет число поддельных сайтов, замаскированных под надежные источники. Переориентация значительной доли населения на дистанционную работу с использованием личных, не всегда достаточно защищенных компьютеров, расширение онлайн-сервисов и торговли также предоставляют террористам новые возможности для поиска доходов за счет хакерских атак и использования мошеннических схем. В еще большей степени проблема обострилась в европейских государствах. Интерполом даже был подготовлен специальный доклад по этим вопросам. Специалисты также отметили новое явление — медикализацию, когда страх заражения инфекцией побуждает людей приобретать онлайн контрафактные и даже несуществующие медицинские товары.

При этом сохраняются приемы финансирования терроризма, закамуфлированные под религиозную благотворительность.

Например, в августе 2020 г. органы безопасности совместно с правоохранительными органами Российской Федерации вскрыли целую сеть финансирования, узлы которой находились в Москве, Подмосковье, Дагестане, Красноярском крае и Ханты-Мансийском автономном округе. Деньги шли в основном в Сирию, на поддержку ИГИЛ. В этот же период в Нижнем Новгороде была задержана группа мигрантов из Таджикистана, направлявших деньги на нужды МТО в Афганистан. Аналогичные задержания прошли в Санкт-Петербурге, Томске, Югре, а уже в нынешнем году — в Новосибирске, Казани, Крыму. В июле 2020 г. Сахалинский областной суд вынес приговор гражданину Узбекистана по статье Уголовного кодекса, предусматривающей ответственность за содействие террористической деятельности в форме финансирования терроризма.

Кибератаки на информационные системы (кибертерроризм). Данное направление включает прямое использование компьютерных ресурсов в качестве средства совершения террористических атак против информационных систем. Под кибертерроризмом, как правило, понимают действия по дезорганизации информационных систем, создающие опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если они совер-

шены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решения органами власти, а также угрозу совершения указанных действий в тех же целях[1]. Орудием кибертеракторов выступает вредоносное программное обеспечение (вирусы, «трояны», программы для массовой рассылки сообщений и т.п.).

Ключевая цель кибертеррористов — системы управления критически важными объектами инфраструктуры (транспорт, атомная энергетика, электросети и т.д.), нарушение работы которых может повлечь значительные негативные последствия. Причем последние не ограничиваются только киберпространством, а затрагивают объекты реального мира, такие как системы жизнеобеспечения городов (электроэнергетические сети, система теплоснабжения), объекты авиа-, морского (речного) и железнодорожного транспорта, атомной энергетики и т.д.

Говоря о кибертерроризме, следует иметь в виду возможную связь исполнителей таких терактов со спецслужбами определенных государств. Другими словами, террористы могут осуществлять кибератаки в интересах третьей стороны против определенного государства в соответствии с полученными директивами, выполняя тем самым за нее «грязную работу».

Выступая на коллегии Федеральной службы безопасности в феврале 2021 г., Президент Российской Федерации В.В. Путин обратился к аудитории: «Особое внимание прошу уделить вскрытию контактов террористических групп и зарубежных спецслужб. Вы это хорошо знаете, к сожалению, все идет в ход, используют и террористов»[2].

В Докладе группы правительственных экспертов ООН A/65/201 также отмечается, что физические лица, группы и организации, включая преступные группы, выполняют посреднические функции в осуществлении подрывной сетевой деятельности от имени других[3]. Для государства — заказчика такой операции это отличный способ избежать ответственности за свои действия. При этом для обеспечения успеха операции оно может передать террористам всю

---

1 *Федоров А.В.* Информационная безопасность в мировом политическом процессе: учеб. пособие. М.: МГИМО, 2006. С. 111.

2 Заседание коллегии ФСБ России // Президент России. 2021. 24 февр. URL: http://www.kremlin.ru/events/president/news/65068 (дата обращения: 12.04.2021).

3 Доклад правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности / Организация Объединенных Наций. Нью-Йорк, 2012. С. 1–10.

необходимую информацию об объекте кибератаки (в том числе полученную разведывательным путем). Нельзя также исключать возможности использования спецслужбами террористов для указанных целей «втемную» посредством организации контролируемых утечек информации и совершения определенных действий.

Еще одной формой кибертерроризма следует считать хакерские атаки на правительственные и корпоративные сайты с целью блокирования их работы либо размещения на них пропагандистской информации.

Экстремистская пропаганда в цифровой среде

Как отмечалось выше, пропаганда выступает одним из ключевых направлений использования ИКТ экстремистами. Согласно Уголовному кодексу РФ под пропагандой терроризма понимается «деятельность по распространению материалов и (или) информации, направленных на формирование у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности» (прим. 1.1 к ст. 205.2).

Выступая на заседании коллегии Генеральной прокуратуры РФ в марте 2021 г., руководитель ведомства И.В. Краснов отметил, что интернет стал одним из основных источников распространения экстремистской идеологии. С его использованием совершается половина соответствующих преступлений. При этом их общее число в 2020 г. возросло почти вдвое. В 2020 г. российскими правоохранительными органами противоправный контент удален с 52 тыс. интернет-ресурсов, заблокирован доступ к 10 тыс. сайтов.

Основными целями пропагандистской деятельности радикалов выступают распространение экстремистской идеологии, популяризация ее среди населения, отдельных социальных групп и лиц, их радикализация, а также подстрекательство к осуществлению террористической и экстремистской деятельности. Пропаганда также может «использоваться в качестве доказательства успешного проведения террористических актов для тех, кто обеспечивает соответствующую финансовую поддержку»[1].

Экстремистские организации стараются привлечь к своей активности и идеологическим концепциям широкое общественное внимание, используя для этого наиболее влиятельные источники массовой информации — СМИ и интернет-ресурсы.

---

[1] *Овчинский В.С.* Криминология цифрового мира: учебник для магистратуры. М.: Норма: ИНФРА-М, 2018. С. 127.

СМИ рассматриваются террористами как важный канал донесения своих устрашающих «посланий» до общества и оказания давления на органы власти. Как отмечает *Б. Накос*, «прибегая ко все более зрелищным и жестоким действиям и таким образом повышая порог насилия, террористы уверены в самом широком освещении своих действий в прессе и общественном внимании»[1]. Именно через СМИ террористы получают неограниченные возможности для воздействия на власть и общественное мнение, проведения массированных информационных атак, что, в свою очередь, является предпосылкой успеха в информационной агрессии, ставшей основным компонентом практически любого террористического акта на всех этапах его осуществления. «Медиатерроризм» порождает и стимулирует хаос, разрушение социальной устойчивости, усиление атмосферы «парализующего пессимизма», усиление общественной напряженности и конфликтности, нарушение нормального функционирования властных структур, подрыв доверия населения к действиям и намерениям власти[2].

Однако законодательные ограничения и редакционная политика СМИ затрудняют информационное освещение терактов и иных преступлений в нужном радикалам ключе и трансляцию их экстремистских идей. По этой причине наиболее мощные террористические и экстремистские организации стремятся создавать и развивать собственные СМИ в пропагандистских целях.

По мере развития интернета именно к нему перешла роль основного канала пропаганды экстремистов. Причиной тому стали мощный рост интернет-аудитории, простота создания и администрирования интернет-ресурсов, отсутствие цензуры, фактор анонимности пользователей, трансграничная передача информации и др. Известный неонацистский ресурс *Stormfront* был создан в США в далеком 1995 г. и считается одним из первых экстремистских сайтов в мире. Однако с той поры уже прошло много времени, и в настоящее время можно говорить о существовании *мощной цифровой экосистемы экстремизма*.

Основным «драйвером роста» экстремистской пропаганды в 2000-е и 2010-е гг. выступали джихадистские террористические организации, прежде всего «Аль-Каида» и ИГИЛ. Последняя вывела террористическую пропаганду на невиданный ранее уровень.

---

1 *North A.* How Media Coverage Influences Terrorism // BuzzFeed. 19 April 2013. URL: http://www.buzzfeed.com/annanorth/how-media-coverage-influences-terrorism (дата обращения: 14.08.2013).

2 *Цыганов В.* Медиа-терроризм. Терроризм и средства массовой информации. Киев: Ника-Центр, 2004. С. 25, 30.

В структуре данной организации в 2010-х гг. функционировал мощнейший медиахолдинг, который производил широкий перечень мультимедийной продукции — видеофильмы, агитационные ролики, аудиозаписи проповедей и нашидов, журналы, буклеты, постеры и т.п.[1] Сочетание грамотно выстроенной идеологической базы нарративов, высококачественного контента и широкой сетки информационных каналов донесения информации до целевой аудитории позволило в свое время ИГИЛ завоевать глобальную популярность и привлечь в свои ряды большое число сторонников со всех частей света. По оценкам, приведенным в ноябре 2015 г. Генеральным прокурором Российской Федерации, в составе ИГИЛ на тот момент воевали выходцы из более чем 100 стран мира.

После военного разгрома ИГИЛ ее пропагандистская активность существенно снизилась. Вместе с тем апробированные ею методики начали воспроизводиться другими террористическими и экстремистскими структурами. Специалисты отмечают активизацию русскоязычного сегмента пропаганды афганского Талибана, ориентированного на молодежь из центральноазиатских государств. Эта тенденция сохраняется. Однако появились и новинки, указывающие на расширение языкового поля пропаганды. Анализ видеоконтента, размещаемого на ресурсах Талибана, позволил выявить пропагандистские видеоролики на узбекском языке и языках других народов, проживающих в государствах Центрально-Азиатского региона. Изготовление видеопропаганды просто поставлено на конвейер. При этом сам видеоряд имеет весьма качественную режиссуру и графику. Особая эстетика «джихадистского Голливуда», как говорят эксперты. Устойчиво присутствует такой формат, как видеоролик-обращение. Это одновременно и пропаганда, и прямой приказ к действию, хотя там и нет конкретных объектов и адресов. Но если человека такое видеообращение чем-то зацепило, он пойдет искать и взрывчатку, и объект. Таким образом, на одно звено — вербовщика — сокращается линейка воздействия (от пропаганды к новообращенному).

Резкую активизацию вербовщиков МТО в социальных сетях и мессенджерах отмечают правоохранительные органы Республики Таджикистан. Здесь акцент делается на призывах к вооруженной борьбе против конституционного строя. В целях организации агитационно-пропагандистской работы против правительства зару-

[1] *Сундиев И.Ю., Смирнов А.А., Костин В.Н.* Информационно-пропагандистская деятельность террористической организации «Исламское государство Ирака и Леванта» // Библиотека криминалиста. 2015. № 1. С. 208–218.

бежными спецслужбами создана телевизионная студия «Садои-мардум» (*Голос народа*). *Данный канал вещает через спутник, его офис находится в Варшаве.*

В конце декабря 2020 г. Талибан распространил в сети 10-минутный фильм под названием «Фатҳи райони Моймай» (*«Покорение района Маймай»*). *Это своего рода видеоотчет об уничтожении в ноябре 2020 г. поста афганской полиции в районе Маймай* (*Верхний Дарваз*) *северной афганской провинции Бадахшан. Однако фильм содержит и прямой месседж — готовность некоторых подразделений Талибана провести аналогичные операции уже «за Пянджем». В нападении под командованием полевого командира Джумы Талбона участвовали не менее 10 граждан Таджикистана, и они не прятали свои лица. Органам безопасности Республики их имена, конечно, были известны. Контрпропагандистские действия не заставили себя ждать. В сети появился видеофильм с участием родителей и близких родственников боевиков с призывами сложить оружие, вернуться и тем самым заслужить прощение на родине.*

В конце 2010-х гг. спецслужбами отмечена активизация правого экстремизма в мире, прежде всего в США и Европе. По данным Глобального индекса терроризма 2020 (Global Terrorism Index 2020) число нападений ультраправых в Северной Америке, Западной Европе и Океании увеличилось с 2014 г. на 250%, а число смертей за тот же период возросло на 709%[1]. Такому всплеску во многом способствовали массированное информационное присутствие и пропаганда праворадикальных сообществ в интернете. Крайне правые наводнили своим экстремистским контентом крупные социальные платформы, а также создали и захватили альтернативные информационные площадки, сформировав тем самым обширную виртуальную экосистему правого экстремизма. Активизации правых экстремистских группировок также благоприятствовало длительное нахождение в тени ИГИЛ и других джихадистских группировок, которым уделялось основное внимание со стороны правоохранительных органов и администрации социальных сетей.

В настоящее время основными звеньями информационной инфраструктуры экстремистов в цифровом пространстве выступают:

1. ***Специализированные экстремистские сайты и платформы***. Данный тип экстремистских ресурсов возник еще в 1990-е гг. (web 1.0) и продолжает использоваться для пропаганды

[1] Institute for Economics & Peace. Global Terrorism Index 2020: Measuring the Impact of Terrorism. Sydney, November 2020 // Vision of Humanity. URL: https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf (дата обращения: 21.01.2021).

радикальной идеологии, освещения повестки дня в выгодном экстремистам ракурсе и распространения призывов к террористической и экстремистской активности своих сторонников. Многие сайты имеют площадки для общения пользователей, обсуждения идей и мнений. Они считаются одним из наиболее уязвимых элементов цифровой экосистемы радикалов, так как их достаточно просто удалить или ограничить к ним доступ (на уровне хостинг-провайдера или оператора связи). Хотя некоторые из них, например ультрапраправый сайт *DailyStormer*, длительное время свободно действовали в США и некоторых западных странах. В России же наиболее известные экстремистские сайты (IslamDin, «Кавказ-центр» и др.) были запрещены и заблокированы.

2. ***Сообщества и аккаунты радикальной направленности в основных социальных сетях***. Они возникли уже в 2000-е гг. с расцветом крупных сетевых ресурсов (Facebook, YouTube, Instagram, «ВКонтакте» и др.) и в настоящее время выступают ключевым звеном массовой экстремистской пропаганды, рассчитанной на широкую аудиторию. В последние годы из-за пропагандистской деятельности ИГИЛ, а затем — праворадикальных сообществ, администрации крупных социальных сетей под давлением властей и общественного мнения начали активно зачищать свои площадки от экстремистского контента и присутствия. Это привело к миграции радикалов на альтернативные площадки.

3. ***Радикальные чаты и каналы в мессенджерах***. С бурным развитием мессенджеров (WhatsApp, Viber, Telegram, Facebook Messenger) в 2010-е годы они стали широко задействоваться террористами и экстремистами для ведения коммуникаций и распространения пропагандистских материалов. Простота использования, удобство групповых каналов и чатов, опции анонимности и шифрование переписки вывели мессенджеры в число ключевых технологических средств экстремистской коммуникации, потеснив по некоторым позициям даже социальные сети. Особенно в этом плане выделяется мессенджер *Telegram*, обладающий повышенными настройками конфиденциальности и возможностью создания тематических каналов (аналог пабликам в социальных сетях). Он стал одним из самых популярных инструментов индивидуального и группового общения террористов и экстремистов, а также распространения пропаганды и призывов к совершению экстремистских акций. Кроме того, в последние годы Telegram стал активно применяться на постсоветском пространстве для организации незаконных протестных акций и массовых беспорядков. Наиболее ярко это проявилось в событиях в Белоруссии 2020–2021 гг., где

данный мессенджер стал главным рупором протеста и координации действий его участников.

В рассматриваемом контексте весьма показательна роль интернет-платформы NEXTA в координировании социальных волнений в Республике Беларусь в течение 2020–2021 гг., которые в дальнейшем получили со стороны правоохранительных органов Республики юридическую оценку как экстремизм, а по некоторым эпизодам — даже как терроризм. Комментируя ситуацию, Е.Г. Пономарева подчеркивает, что основным информационно-коммуникативным ресурсом дестабилизации ситуации в республике стали именно оппозиционные телеграм-каналы (прежде всего, платформы NEXTA). Массовость (впервые в истории Беларуси протестные демонстрации на пике собирали до 150 тыс. чел. и более) протестов была обеспечена предшествующей (в течение нескольких месяцев) работой в социальных сетях и мессенджерах по формированию негативного отношения к власти и уверенности в том, что она падет, как только толпа выйдет на улицу. Е.Г. Пономарева выделила несколько направлений противоправной деятельности, координировавшихся данным цифровым ресурсом: массовые протестные акции с применением сцепок и провоцированием ОМОНа; пикеты солидарности с «политзаключенными»; пикеты солидарности диаспор (28 июня они прошли в 14 городах США, крупных городах Германии и Польши, в столицах ряда европейских стран и в Тбилиси); флешмобы разных форматов (цепи солидарности, вело- и автопробеги; шествия домохозяек с кастрюлями); аплодисменты как акция расположения и одновременно устрашения силовиков; челленджи[1]. *К инструментам дестабилизации (матрицы влияния) специалисты обоснованно отнесли помимо ряда бумажных и цифровых оппозиционных средств массовой информации также социальные медиа — паблики, телеграм-каналы, целевые социальные сети, сообщества блогеров (в том числе цифровые ресурсы «Беларусь головного мозга», «Арт-Сядзіба», паблик sinbal.by и т.д.)*[2].

---

[1] См. подробнее: *Пономарева Е.Г.* Протестное движение в Белоруссии: эволюция, технологии, символы // Деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя, как угроза государственной и общественной безопасности стран СНГ: сб. науч. ст. участников совместного заседания Научно-консультативного совета при АТЦ СНГ и Ученого совета АНО «Научно-исследовательский институт проблем безопасности СНГ». М., 2021. С. 70–79.

[2] Аналитический центр «Агентство социального инжиниринга». URL: https://sea.com.ru/ru.

В данном контексте представляется важной дифференциация конкретных фрагментов социальных волнений. По этому поводу *А.Ю. Маруев* сделал справедливое замечание: «Во многих случаях формы "протестной активности" не связаны с нарушением законности. В то же время любая из указанных форм "протестной активности" может принять радикальный характер, угрожать общественному порядку, дестабилизировать жизнедеятельность общества и государства и быть использована деструктивными силами для провоцирования массовых волнений, беспорядков и актов гражданского неповиновения»[1].

4. ***Экстремистские сообщества и аккаунты на альтернативных интернет-ресурсах***. В результате проведения последовательной, согласованной политики национальных властей и администрации сетевых ресурсов по очистке интернет-платформ от экстремистского присутствия идеологи и сторонники радикальных взглядов начали активно искать себе новые убежища. При этом использовались две стратегии: создание новых самостоятельных платформ или захват («колонизация») существующих. Например, правые экстремисты на Западе после их вытеснения из крупных социальных сетей и мессенджеров начали активно задействовать тематические экстремистские площадки (Gab, Voat, 8Chan) и захваченные платформы (Reddit, 4Chan, Discord). Например, ультраправый имиждборд 8Chan был использован в 2019 г. несколькими правыми экстремистами для размещения «манифестов», в которых они объясняли свои действия и призывали единомышленников совершать нападения. Это касалось нападений 15 марта в Крайстчерче (Новая Зеландия), 27 апреля в Пауэе (Калифорния, США) и 3 августа в Эль-Пасо (Техас, США).

В России после действий властей по противодействию использованию экстремистами мессенджера Telegram отмечались попытки экстремистских элементов исламистского и праворадикального толка перейти на альтернативные мессенджеры *Signa*l, *Threema*, *TamTam* и др.

---

[1] *Маруев А.Ю.* Анализ факторов протестной активности населения в современной России и меры по их минимизации // Деятельность террористических и экстремистских организаций, направленная на насильственное изменение конституционного строя, как угроза государственной и общественной безопасности стран СНГ: сб. науч. ст. участников совместного заседания Научно-консультативного совета при АТЦ СНГ и Ученого совета АНО «Научно-исследовательский институт проблем безопасности СНГ». М., 2021. С. 89–90.

5. ***Закрытые группы, каналы и чаты на интернет-ресурсах***. В западной литературе для обобщенного наименования данных коммуникационных каналов используется термин «DarkSocial», который можно перевести как «темные социальные сети». В маркетинге им обозначаются платформы, передачу контента через которые трудно отслеживать. К ним относятся, например, электронные письма, смс-сообщения и зашифрованные чаты. В контексте темы экстремизма он обычно применяется при описании используемых экстремистами для коммуникации каналов, которые сложно анализировать с помощью традиционных инструментов анализа социальных медиа[1]. Экстремистами преимущественно используются закрытые чаты и паблики в мессенджерах (WhatsApp, Telegram, Discord, Signal), доступ к которым осуществляется по личному приглашению, рекомендации других участников или после предоставления доказательств лояльности. Такие площадки чаще всего используются для обсуждения радикальных идей, координации и подготовки коллективных акций, а также для планирования нападений.

Авторы профильных аналитических исследований справедливо отмечают, что цифровые ресурсы следует рассматривать как высокотехнологичный инструмент социального инжиниринга. Экстремистским и (или) террористическим тот или иной цифровой ресурс делает содержание наполняющего его контента.

Вербовка и иные способы вовлечения в террористическую и экстремистскую деятельность в цифровой среде

Цифровая среда открыла экстремистам широкие возможности для вовлечения в противоправную деятельность новых участников. Традиционным способом такого вовлечения выступает вербовка — вхождение в контакт и последующее общение экстремиста с определенным лицом или группой лиц с целью привития им радикальных взглядов, убеждения вступить в ряды террористической или экстремистской организации либо стимулирования определенных действий.

Деятельность террористических и экстремистских организаций по привлечению новых рекрутов осуществляется путем как непосредственного (личного) контакта вербовщика с вербуемым, так и дистанционного, когда вербовщик (он может находиться на тер-

[1] *Davey J., Ebner J.* The Great Replacement: the violent consequences of mainstreamed extremism // Institute for Strategic Dialogue. 2019. URL: https://www.isdglobal.org/isd-publications/the-great-replacement-the-violent-consequences-of-mainstreamed-extremism (дата обращения: 05.09.2020).

ритории третьих стран) входит в контакт при помощи сети Интернет и мобильной связи. Причем вторая форма становится доминирующей.

Вербовка в интернете ведется как в отношении широкого круга лиц, в котором могут найтись сторонники радикальных идей, так и таргетированно, в адрес конкретных целевых групп и личностей. Вербовщику только необходимо отыскать в виртуальном пространстве лиц, которые согласно имеющимся социально-психологическим установкам способны войти в состав группы[1]. Этому способствует публикация пользователями социальных сетей большого объема сведений, характеризующих их индивидуально-личностные особенности: убеждения, взгляды, сферу интересов и т.п.

Наибольшую активность эмиссары радикальных организаций проявляют в самых популярных социальных сетях, таких как «ВКонтакте», «Одноклассники», «Facebook», «Instagam», где происходят подбор и первичное общение с возможными кандидатами. Для общения вербовщики также активно используют мессенджеры: «Viber», «WhatsApp», «Telegram», «Threema» и др.

Вербовочная деятельность эмиссаров террористических и экстремистских организаций осуществляется с соблюдением правил конспирации. В частности, они соблюдают осторожность при общении в малознакомых аудиториях, используют для модемного соединения SIM-карты операторов телефонной связи, оформленные на третьих лиц, при вводе личных данных сообщают о себе ложную информацию (Ф.И.О., возраст, место жительства), общение по вопросам оказания пособнической помощи радикальным организациям ведут только в личной переписке, для сокрытия IP-адресов вход в социальные сети осуществляют через VPN или прокси-серверы и т.п.[2]

По мнению специалистов компании «Крибрум», для привлечения подростков в экстремистские и другие деструктивные группы в цифровой среде применяются так называемые «воронки вовлечения». На верхнем уровне такой воронки действуют мно-

---

[1] *Румянцев А.А.* Характеристика современных проявлений терроризма // Материалы VII Региональных экспертных консультаций представителей органов безопасности, специальных служб и правоохранительных органов государств — участников СНГ по борьбе с терроризмом и иными насильственными проявлениями экстремизма и расширенного пленарного заседания Научно-консультативного совета при АТЦ СНГ: сб. мат-лов. СПб.: Русь, 2017. С. 97.

[2] *Кочубей М.А., Мареев П.Л., Смирнов А.А., Сутормина Е.В.* Профилактика терроризма и экстремизма в молодежной среде. СПб.: Русь, 2018. С. 49.

гочисленные группы широкого охвата, содержащие базовую информацию и пропаганду темы. Далее следуют группы более узкой тематики для тех, кто «созрел». В них уже имеются специальные условия вступления и предполагается выполнение заданий участниками. На следующем уровне действуют частные группы, которые отличают четкая тематика и наличие своей субкультуры. И на последнем этапе уже происходит приватное общение с лицом и выполнение им действий в реальном мире[1].

Пропаганда терроризма и вербовка новых боевиков продолжаются и в период пандемии[2]. Привлечению рекрутов в ряды террористических организаций не только по религиозным, но и по финансовым мотивам способствуют такие факторы, как безработица и сокращение доходов. К числу последствий сложившейся ситуации, потенциально влияющих на пополнение ресурсной базы терроризма, следует отнести обращение испытывающих финансовые трудности граждан к нетрадиционным или нелицензированным заимодателям, включая преступные и террористические группировки. Невозможность возврата займа сделает должника их заложником, готовым для погашения долга совершить иные, включая противоправные, действия в их интересах.

Современные информационные технологии способствовали развитию не только дистанционных технологий вербовки в террористические и экстремистские организации, но и широкому распространению *бесструктурных способов вовлечения в террористическую и экстремистскую деятельность*. Термин «бесструктурные» в данном контексте означает возможность удаленного формирования и стимулирования противоправной активности индивидов

---

1 *Самосват О.* Деструктивные течения в социальных медиа и способы их выявления. Доклад на форуме «Цифровая гигиена. Молодежь в сети». 28 марта 2019 г.

2 Данной проблеме посвящен ряд специальных исследований и зарубежных авторов. Однако акцент в них сделан на возросшей активности ультралевых и ультраправых экстремистов. См. например: *Weimann G., Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace // International Institute For Counter-Terrorism URL: https://www.ict.org.il/Article/2528/The_Virus_of_Hate#gsc.tab=0; *Wither J.K. T*he COVID-19 Pandemic: A Preliminary Assessment of the Impact on Terrorism in Western States // The George C. Marshall European Center for Security Studies. URL: https://www.marshallcenter.org/en/publications/occasional-papers/covid-19-pandemic-preliminary-assessment-impact-terrorism-western-states-0; *Wallner C., White J.* The Far-Right and Coronavirus: Extreme Voices Amplified by the Global Crisis. URL: https://rusi.org/commentary/far-right-and-coronavirus-extreme-voices-amplified-global-crisis.

и групп без формального их вхождения в состав террористических и экстремистских структур.

В основе таких способов воздействия лежит *механизм краудсорсинга* (англ. *crowdsourcing*; *crowd* — «толпа» и *sourcing* — «использование ресурсов») — привлечение к решению определенных задач широкого круга лиц на добровольных началах с использованием информационно-коммуникационных технологий. В классическом случае краудсорсинг — это схема, по которой задания посредством интернета передаются заранее неизвестной группе исполнителей («толпе») в форме открытого конкурса[1].

На первом этапе эволюции интернета (web 1.0) появились многочисленные ресурсы радикальной направленности, на которых содержались литература и публикации экстремистского характера, инструкции о способах изготовления оружия и взрывных устройств, способах совершения терактов и силовых действий в отношении сотрудников правоохранительных органов и т.п. Такого рода информация и раньше распространялась через подпольные издания, однако именно с появлением интернета доступ к ней получили миллионы пользователей.

Дальнейшее повышение качества и содержания экстремистских ресурсов, включающих профессионально снятые видеофильмы и ролики, высококлассные печатные издания, пособия и инструкции, создало основу для процесса саморадикализации, когда индивид приобретает экстремистские взгляды посредством потребления экстремистского контента в сети, а также самостоятельно «осваивает» методы и средства осуществления террористической и экстремистской деятельности. Развитие мобильной связи и сетевых интернет-технологий (web 2.0) значительно расширило возможности распространения экстремистского контента любым пользователем, а также обеспечило сторонников радикальных взглядов доступными инструментами дистанционного влияния в глобальном масштабе.

В своей совокупности описанные ИКТ обеспечили осуществимость дистанционного бесструктурного и бесконтактного управления как отдельными индивидами, так и большими массами людей (толпой), что было использовано идеологами радикальных организаций для инспирирования террористической и экстремистской деятельности[2].

---

[1] *Беленький А.* Многоликий краудсорсинг // КомпьютерПресс. 2011. № 10. С. 30–36.

[2] *Сундиев И.Ю., Смирнов А.А., Андрюхин Н.Г.* Бесструктурные и бесконтактные способы вовлечения молодежи в террористическую и экстремистскую деятельность // Научный портал МВД России. 2018. № 2. С. 53.

Прежде всего, технологии дистанционного управления были задействованы при организации коллективных акций «умной толпы», включая протестные акции и массовые беспорядки. Отличительными чертами «умной толпы» являются не только новые способы ее формирования (для возникновения «традиционной толпы» нужен «шоковый стимул» — внезапное событие, прямо затрагивающее жизненные интересы участников; «умная толпа» направленно формируется за счет продолжительного диалога в сетевых ресурсах и средствах массовой коммуникации[1]), но и активная роль каждого ее участника при планировании и реализации проводимых акций (участие в обсуждении замысла, оперативная координация, информационное освещение).

Ярким примером использования социальных сетей и сервисов микроблогов для массового вывода людей на улицы является так называемая «Арабская весна». В своей книге «Революция 2.0» один из организаторов революционных выступлений в Египте *Ваэль Гоним* описал использованную методику мобилизации общественной поддержки политического протеста через Facebook, включавшую несколько стадий. «На первой стадии убеждаешь людей присоединиться к странице и читать записи. На второй подталкиваешь их взаимодействовать с контентом, ставя “лайки” и комментируя. На третьей — принимать участие в онлайновых кампаниях страницы и самим поставлять контент. На четвертой и последней стадии люди выходят на улицы»[2].

Другим направлением применения краудсорсинговых технологий в экстремистской и террористической деятельности выступает ***стимулирование деструктивной активности со стороны отдельных неперсонифицированных лиц***. В отличие от предыдущего направления, которое реализуется за счет массового участия граждан, оно носит более «приватный» характер и предполагает индивидуальное исполнение. Общим же для этих форм является то, что вовлечение лица в противоправную деятельность происходит без «формального» и «непосредственного» вхождения в организационные структуры радикальных организаций и объединений.

Бесструктурные способы вовлечения в террористическую деятельность лежат и в основе такой современной ее формы, как *терроризм одиночек*. Под террористом-одиночкой обычно понимается

---

1 *Сундиев И.Ю., Смирнов А.А.* Теория и технологии социальной деструкции (на примере «цветных революций»): монография. М.: Русский биографический институт, Институт экономических стратегий, 2016. С. 259.

2 *Гоним В.* Революция 2.0: Документальный роман: пер. с англ. СПб.: Лениздат: Команда А, 2012. С. 93.

лицо, формально не входящее в состав ячейки террористической организации и самостоятельно совершающее террористический акт вследствие саморадикализации. Террористическая активность индивида в данном случае является спонтанным актом, следствием потребления экстремистского контента в сети и виртуального общения в многочисленных радикальных каналах и группах, в ходе которого он «заражается» идеологией экстремизма и выходит на путь террора.

Этому предшествует активная пропагандистская кампания самой террористической и экстремистской организации, обеспечивающая ей привлечение внимания широкой аудитории и получение известности. На следующем этапе некоторым представителям привлеченной «паствы» даются указания о том, что они должны «делом» доказать свою верность идеям организации и подтвердить свою собственную решительность и храбрость. Форма этих указаний может быть различной: от размещения на видеохостинге обращения лидера террористической организации до распространения через тематические каналы в мессенджерах пропагандистских постов с соответствующими призывами.

Так, в выпущенном летом 2016 г. проигиловской хакерской группой «Объединенный киберхалифат» («United Cyber Caliphate») пропагандистском постере был размещен прямой призыв к совершению убийств «неверных» в качестве «мести за мусульман»: «О, львы-одиночки, разбросанные по всему миру. Убивайте крестоносцев, где бы вы их не встретили. За их войну против Ислама и муджахидов. Убивайте их решительно. Убивайте их жестоко».

Для совершения одиночных атак сторонникам ИГИЛ было рекомендовано использовать любые доступные средства — ножи, топоры, автотранспортные средства, огнестрельное оружие и т.д. В этом, на наш взгляд, кроется одна из причин всплеска террористических атак в Европе, поскольку такой подход заметно упрощает процесс приготовления к совершению преступления и существенно расширяет круг его потенциальных исполнителей (ведь кухонный нож или топор, в отличие от взрывчатки, может приобрести и использовать любой желающий). Основной аудиторией пропагандистской кампании ИГИЛ на Западе стала молодежь из миграционных волн («беженцев»), затопивших Европу в 2014–2017 гг.

Как отмечают эксперты, «просмотр материалов запрещенного в России ИГ и онлайн-радикализация в большинстве случаев не влияют на поведение в реальной жизни. Страх погибнуть или быть арестованным пересиливает все блага, которыми джихадисты

прельщают потенциальных мучеников. Поэтому их "амалии" носят куда меньшие масштабы: вместо взрывов — раскрашенные автомобили, вместо казней — травля популярных в интернете блогеров... Лишь отдельные личности из числа подписчиков подобных каналов рискуют последовать методичкам, остальные же продолжают оставаться "опасными" лишь на просторах сети. И отчаянно нуждаются в примере, который их "вдохновит"...»[1].

В России за последние годы также были совершены несколько нападений «волками-одиночками» (*террористический акт на Джемикентском посту ГИБДД в Дагестане 15 февраля 2016 г., нападение на пост ДПС в Московской области 17 августа 2016 г., ножевая атака в Сургуте 19 августа 2017 г., расстрел из охотничьего оружия прихожан православной церкви в г. Кизляр Республики Дагестан 18 февраля 2018 г.*).

Наряду с совершением террористических актов и иных нападений, формой бесструктурного участия лиц в экстремистской деятельности может выступать проведение ими пропагандисткой деятельности. Наиболее успешно данную форму бесконтактного вовлечения использовала МТО ИГИЛ. Как показал исследователь *Ч. Уинтер* на основе анализа методического документа ИГИЛ по пропаганде под названием «Медиа-оператор, ты тоже моджахед!», данная террористическая организация в агитационной работе существенное внимание уделяет стимулированию своих сторонников к ведению индивидуальной пропаганды, которая позиционируется как одна из самых значимых форм джихада. В указанном документе говорится: «Братьям медиа-операторам ИГ: вы должны знать и быть убежденными в том факте, что ваша работа — это тоже джихад во имя Аллаха, и что вы, выполняя ее, являетесь муджахидами, следующими по пути Аллаха». Далее следует обсуждение критических аргументов против такой формы «джихада»: «Некоторые критикуют "медиа-операторов" за то, что они ведут словесный джихад, сидя на диванах в прекрасных домах. Наоборот, "медиа-операторы" находятся на передовой, в самом сердце войны, в самом пекле битвы. Плечом к плечу со своими братьями, они сражаются с врагами Аллаха в этом мире, высоко поднимая знамя джихада. Они преломляют хлеб свой с ними, повсюду сопровождают их, спят на голой земле рядом с ними. ...Не будет преувеличением сказать,

[1] Мамкины шахиды. Почему российские подростки становятся террористами // Лента.ру. 2017. 7 апр. URL: https://lenta.ru/articles/2017/04/07/diwan/ (дата обращения: 09.04.2017).

что медиа-оператор — это мученик без “пояса шахида”. Этот титул они заслужили»[1].

Как справедливо резюмирует сам автор, «обещание активного, но не представляющего большого риска участия в джихаде оказалось исключительно привлекательной идеей для многих тысяч людей во всем мире»[2]. Именно она, в сочетании с мощной пропагандистской машиной террористической организации, позволила сформировать децентрализованную сеть распространения радикальной исламистской идеологии в глобальном масштабе.

Использование глубоких фейков в террористической и экстремистской деятельности

Понятие «глубокие фейки» (*deepfakes*) образовано от терминов «глубокое машинное обучение» (*deeplearning*) и «фейки» (*fakes*). Его происхождение связывается с одноименным ником пользователя интернет-платформы «Reddit», который заявил в 2017 г., что использует технологии машинного обучения для того, чтобы имплантировать изображения лиц знаменитостей в порнографические видео.

«Глубокие фейки» (deepfakes) представляют собой технологии искусственного синтеза человеческого изображения, основанные на использовании нейросетей и искусственного интеллекта, позволяющие создавать высокореалистичные фото- и видеоизображения людей либо производить модификацию фото-, аудио- и видеоматериалов[3]. К дипфейкам относятся также методы создания аудиофальшивок, говорящих голосом нужного человека.

Глубокие фейки являются продуктом достижений в формах искусственного интеллекта (ИИ), известных как «глубокое обучение» (deeplearning), в котором набор алгоритмов, называемых «нейронными сетями», обучается понимать правила и воспроизводить паттерны (модели) путем обработки больших данных (Google, например, использовала эти технологии для развития мощных

---

1 *Winter Ch.* Media Jihad: The Islamic State’s Doctrine for Information Warfare. International Centre for the Study of Radicalisation and Political Violence, 2017.

2 Ibid.

3 *Смирнов А.А.* «Глубокие фейки». Сущность и оценка потенциального влияния на национальную безопасность // Свободная мысль. 2019. № 5. С. 63.

алгоритмов классификации изображений для своей поисковой системы)[1].

Хотя дипфейки представляют собой лишь новую технологию создания подделок, уникальность им придает сочетание двух свойств: 1) использование убедительного и популярного видеоформата; 2) сложность обнаружения фальшивых видео, изготовленных с помощью данной технологии. В отличие от фотоизображений, возможность искусственной коррекции которых широко известна и применяется многими пользователями социальных сетей, видеозаписям люди склонны доверять гораздо больше. Сам формат видео позволяет зрителям выступать непосредственными очевидцами события, избавляя их от необходимости решать, стоит ли доверять чьему-либо рассказу о нем, что повышает его убедительность.

Поэтому при создании высококачественного вирусного deepfake-видео оно способно распространяться с огромной скоростью в глобальном масштабе, особенно в сочетании с целенаправленными усилиями по его продвижению в сети. При этом люди будут склонны ему верить, поскольку зрительно не заметят каких-то признаков подлога, а официальная реакция властей и СМИ не всегда будет в состоянии опровергнуть содержащуюся в нем информацию. В любом случае она будет приходить с задержкой, когда вирусная эпидемия глубокого фейка уже запущена.

В этой связи вполне справедливым является вывод специалистов компании *CyberCube* о том, что «вскоре дипфейки коренным образом изменят ландшафт киберугроз»[2].

Эксперты в один голос заявляют о скором широком применении глубоких фейков, в том числе и в противоправных целях. В первую очередь данными технологиями постараются воспользоваться мошенники и иные преступные элементы. Однако, по нашему мнению, дипфейки получат распространение прежде всего в экстремистской деятельности.

Террористические и экстремистские организации ведут активную пропаганду в информационном пространстве, используя возможности социальных сетей и мессенджеров. Им традиционно не доставало ресурсов для изготовления и распространения фальшивых, но правдоподобных аудио-, фото- и видеоматериалов. По-

---

1 *Chesney R., Citron D.* Deepfakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics // Foreign Affairs. 2019. January/February. P. 148.

2 *Ларина Е., Овчинский В.* Криминальная жизнь дипфейков // Завтра. 2021. 22 апр. URL: https://zavtra.ru/blogs/kriminal_naya_zhizn_dipfejkov (дата обращения: 22.03.2021).

этому они, несомненно, попытаются задействовать технологии глубоких фейков в своих пропагандистских кампаниях.

Прежде всего, они будут стремиться изготовить провокационные фальшивые видео, способные вызвать серьезный резонанс в нужной целевой аудитории. Это могут быть кадры расстрела мирных жителей военнослужащими, жестоких пыток в отношении лиц, подозреваемых в причастности к терроризму или экстремизму, совершения оскорбительных действий в отношении объектов религиозного культа и т.п. Вброс подобных видео будет преследовать цель стимулирования быстрой и острой общественной реакции — провоцирования массовых беспорядков, разжигания ненависти и провоцирования насилия в отношении определенных лиц или социальных групп.

Вполне очевидно, что идеальной почвой для спекуляций и подстрекательской пропаганды радикалов в странах Содружества будут выступать имеющиеся межконфессиональные, межнациональные и социальные трения и конфликты общегосударственного или локального масштаба. В подобных условиях умело сконструированное фейковое видео может оказаться «детонатором» мощных информационного и социального взрывов, локализовать последствия которых будет достаточно сложно. Свою роль здесь сыграют характерные для психологии толпы возбужденность и следование эмоциональным призывам, нежели рациональным доводам.

В качестве отдельного направления возможного использования глубоких фейков экстремистами следует выделить их применение для дискредитации деятельности правоохранительных органов. Убедительные и эмоциональные видеозаписи «беспредела», якобы творимого «силовиками» (например, фальшивые видео жестокого избиения полицией подростков — участников протестных акций), способны сильно всколыхнуть население либо изменить общественное мнение в отношении правоохранительных органов.

Это будет особенно ярко проявляться в моменты действий силовых структур по пресечению незаконных публичных акций или массовых беспорядков, о чем убедительно свидетельствует пример событий Евромайдана на Украине периода 2013–2014 гг. С самого начала протестных акций в г. Киеве против сил правопорядка была развязана массированная информационная кампания по их дискредитации в украинских и мировых СМИ и на интернет-ресурсах. Ее основными целями было формирование негативного общественного мнения о сотрудниках полицейского отряда «Беркут» и внутренних войск Украины как силовом инструменте «прогнившего и коррумпированного режима» и оправдание действий участ-

ников протестных акций, включая применение насилия в отношении служб правопорядка.

Помимо провоцирования быстрых общественных реакций следует предположить возможность применения глубоких фейков и в более продолжительных пропагандистских кампаниях террористических и экстремистских организаций для продвижения ими своих главных нарративов. Например, они смогут производить и распространять в информационном пространстве фейковые видеозаписи выступлений ликвидированных лидеров и идеологов террористов, якобы «чудом уцелевших и случайно обнаруженных», вложив в их уста любой нужный текст, либо, напротив, вставлять в пропагандистские экстремистские видео фальшивые фрагменты заявлений политических деятелей, которые спровоцируют негодование среди радикальных сторонников.

* * *

В настоящем материале рассмотрены основные проявления цифрового терроризма и экстремизма в современном мире. Радикалы продемонстрировали способность быстро адаптироваться к новым достижениям в сфере ИКТ и брать их себе на вооружение. Вместе с тем время «дикого интернета» давно прошло — власти и провайдеры интернет-услуг научились эффективно выявлять и зачищать элементы экстремистской цифровой инфраструктуры, вынуждая их операторов постоянно искать себе новые убежища. В среднесрочной перспективе экстремисты продолжат активную пропагандистскую и вербовочную работу в социальных сетях и мессенджерах, а также будут стараться задействовать новые ИКТ, связанные с технологиями ИИ, системами виртуальной и дополненной реальности.

Решать задачи, связанные с предупреждением и пресечением использования цифровых технологий в экстремистской и террористической деятельности, возможно только путем задействования всего арсенала сил, средств и методов ОРД.

А.А. Смирнов

О знании тенденций развития правых движений на Западе и их цифровом обеспечении для организации работы оперативных подразделений Российской Федерации

Терроризм и экстремизм остаются в числе ключевых глобальных геополитических рисков и угроз международной безопасности. В первые два десятилетия XXI в. о себе громко заявил джихадистский терроризм, квинтэссенцией которого можно считать создание и деятельность международной террористической организации «Исламское государство» (ИГИЛ), контролировавшей значительную часть территорий Сирии и Ирака и основавшей на них свой псевдохалифат. Помимо этого, «Аль-Каида», ИГИЛ и другие исламистские группировки совершили серию громких террористических атак в западных странах, включая теракты 11 сентября 2001 г. в США, теракты 11 марта 2004 г. в Мадриде, 7 июля 2005 г. в Лондоне и 13 ноября 2015 г. в Париже, а также каскад более мелких террористических нападений в европейских странах в 2015–2020 гг.

Эта ситуация потребовала согласованных усилий всего мирового сообщества, концентрации ресурсов правоохранительных органов и общественных институтов стран Запада для противодействия вызову джихадистского терроризма. Однако в это время экстремистская угроза начала выкристаллизовываться на противоположном фланге политического спектра — правом. По данным «Глобального индекса терроризма 2020» (*Global Terrorism Index 2020*) число нападений ультраправых в Северной Америке, Западной Европе и Океании увеличилось с 2014 г. на 250%, а число смертей за тот же период — на 709%[1].

Отчасти это вызвано реакцией на террористические посягательства на Запад со стороны исламистских радикалов (движение

[1] Institute for Economics & Peace. Global Terrorism Index 2020: Measuring the Impact of Terrorism. Sydney, November 2020 // Vision of Humanity. URL: https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf (дата обращения: 21.01.2021).

контрджихада). Хотя глубинные причины роста правого радикализма были связаны с процессами усиления роли ислама в мире и увеличения доли населения из арабских и африканских государств в Европе вследствие мощных миграционных процессов, которые стали восприниматься как экзистенциальная угроза Западу. В США, минимально затронутых миграционным кризисом, пробуждение ультраправых было детерминировано в большей степени внутренней социальной и политической динамикой. Избрание Дональда Трампа президентом США в 2017 г. ознаменовало собой победу консервативных сил Америки, радикальное крыло которых представлено широким спектром крайне правых движений.

Значимую роль в консолидации и укреплении глобального ультраправого сообщества сыграла цифровая среда, открывшая невиданные ранее возможности для распространения радикальной идеологии и общения с единомышленниками в мировом масштабе. Крайне правые наводнили своим экстремистским контентом крупные социальные платформы, а также создали и захватили альтернативные информационные площадки, сформировав тем самым обширную виртуальную экосистему правого экстремизма. Изменившееся цифровое пространство, в котором торжествуют постправда, фейковые новости и эхо-камеры, повысило уязвимость самого общества к воздействию ультраправых нарративов.

Резонансные террористические атаки в Норвегии в июле 2011 г. и в Новой Зеландии в марте 2019 г., совершенные ультраправыми экстремистами Брейвиком и Таррантом, потрясли Западный мир и заставили спецслужбы обратить пристальное внимание на угрозу правого радикализма. В ежегодных докладах Государственного департамента США и Европола по терроризму (*Country Reports on Terrorism* и *EU Terrorism Situation and Trend report*) прослеживается алармизм в оценках растущей угрозы правового экстремизма в странах Западного мира.

Задачами настоящей статьи являются анализ тенденций и направлений развития правого экстремизма в США и Европе, его идеологической базы, а также изучение инфраструктуры и методов ультраправой пропаганды в современной цифровой среде. Данные знания представляют практическую значимость для работы оперативных подразделений правоохранительных органов России по причине как использования экстремистами схожих средств и методов работы в цифровой среде, так и присутствия ячеек некоторых западных ультраправых движений в нашей стране.

Отметим, что в предмет нашего исследования не будут входить проявления правого экстремизма в государствах — участниках СНГ

и иных странах постсоветского пространства, поскольку они в значительной степени обладают качественно иной спецификой.

1. Понятие и генезис правого экстремизма в странах Запада

Правое направление экстремизма охватывает совокупность радикальных идеологий и насильственных действий, в основе которых лежит представление о господстве определенной национальности или расы, которой угрожают представители иных рас и национальностей, для защиты от которых оправдано применение насилия.

В соответствии с подходом Каса Мадде (Cas Mudde) радикальными правыми (*Extreme-right*) считаются группы и отдельные лица, которые имеют по крайней мере три из следующих пяти признаков: национализм, расизм, ксенофобия, антидемократические убеждения и поддержка сильной государственной пропаганды[1]. Крайне правые группы, как правило, также авторитарны, но зачастую с элементами популизма, и исторически были антикоммунистическими, хотя эта характеристика стала менее заметной после окончания холодной войны[2].

Ключевым понятием в праворадикальном экстремизме является *супрематизм* — идея о том, что определенная группа людей, объединенная общими чертами (национальностью, расой, культурой и т.д.), имеет превосходство над остальными людьми. Осознавая свое превосходство, данная группа считает своим естественным правом доминировать над остальной частью населения[3].

Классическим проявлением правого экстремизма в XX в. выступали фашизм и нацизм, получившие государственный статус и приведшие человечество к новой мировой войне.

Фашизм — общественно-политическое движение и идеология крайне правого толка, а также соответствующая им форма государственного правления. Фашизм как идеология основан на воинствующем национализме, социальном дарвинизме, корпоративизме, расизме, милитаризме, решительном неприятии либерализма, социал-демократии и коммунизма[4].

Нацизм (*национал-социализм*) — экстремистское националистическое движение в Германии 1919–1945 гг., которое с 1920 г. воз-

---

1 Cas Mudde, The Ideology of the Extreme Right. Manchester University Press, 2000.

2 Global Terrorism Index 2020.

3 TE-SAT 2020.

4 Фашизм // Большая российская энциклопедия. URL: https://bigenc.ru/world_history/text/4706908 (дата обращения: 12.08.2020).

главлялось Национал-социалистической немецкой рабочей партией (НСДАП) под руководством А. Гитлера, опора нацистского режима в Германии в 1933–1945 гг. Нередко нацизм считается радикальной формой фашизма. Национал-социализм трактовал историю как непрерывную борьбу народов за выживание, за защиту и расширение необходимого им «жизненного пространства». Конечным результатом этой борьбы должно быть установление мирового господства сохранивших «расовую чистоту» и потому превосходящих другие народы в биологическом отношении арийцев — немцев и родственных им германских народов. Война рассматривалась как естественное состояние человечества, законное и, в конечном счете, единственно возможное средство утверждения мирового лидерства «народа-господина». Залогом победы в этой борьбе объявлялись консолидация немецкой нации под руководством ее вождя — «фюрера», очищение нации от «расово чуждых» и «неполноценных» элементов и укрепление ее «физического здоровья»[1].

Нюрнбергский трибунал 1946 г. раскрыл всему миру детали ужасающих преступлений, совершенных нацистами, их союзниками и приспешниками под знаменами человеконенавистнической концепции превосходства и исключительности. Нацизм, равно как и любые родственные ему идеи и концепции ненависти по расовому, религиозному или другим признакам, были объявлены международным сообществом вне закона[2].

Однако разгром фашизма и его осуждение не повлекли за собой его полного искоренения. Спустя короткое время после окончания Второй мировой войны он снова поднимает голову в Европе и других странах мира. Идеологии политических или общественных движений, возникших после Второй мировой войны, исповедующих национал-социалистические или близкие к ним взгляды либо объявляющих себя последователями НСДАП, стали именоваться *неонацистскими*. Неонацизм заимствует элементы из нацистской доктрины, в том числе шовинизм, фашизм, ксенофобию и антисемитизм. Радикальным неонацистам свойственна приверженность насильственным действиям, вплоть до террористических атак.

Неонацистов отличает ненависть к представителям «небелых» рас, особенно к евреям, которые рассматриваются ими в качестве «архитекторов» мультирасового мирового порядка, где исчезают

---

[1] Национал-социализм // Большая российская энциклопедия. URL: https://bigenc.ru/world_history/text/2252826 (дата обращения: 12.08.2020).

[2] Неонацизм — опасный вызов правам человека, демократии и верховенству права: доклад МИД России. М., 2016.

все нации и традиции перед финальным «захватом мира». В неонацистской среде широко представлена идея «священной расовой войны» (*PaXoBA*, от англ. *Racial Holy War*) планетарного масштаба. Неонацисты также нетерпимо относятся к левым политическим силам, стоящим на позициях интернационализма[1].

Сторонники неонацизма идеализируют фашистское прошлое и активно используют в своей деятельности нацистскую символику и атрибутику, образы лидера Третьего Рейха Адольфа Гитлера. Многие неонацисты используют символику в виде кельтского, мальтийского креста или свастики (включая такую ее разновидность, как «черное солнце»). Последователи данной идеологии применяют нацистское приветствие «Зиг хайль!» (нем. *Sieg Heil!* — «Да здравствует победа!», или «Слава победе!») в сочетании со вскинутой прямой правой рукой с открытой ладонью, а также цифровое обозначение «14/88».

В определении правого экстремизма, используемом Европолом, указывается такая его значимая черта, как *ненависть к меньшинствам*. В Докладе TE-SAT 2020 отмечается, что «правые экстремистские идеологии питаются различными субкультурами ненависти, обычно борясь против разнообразия в обществе и равных прав меньшинств. Правым экстремистам обычно присущи расизм, авторитаризм, ксенофобия, женоненавистничество и враждебность по отношению к лесбийским, гомосексуальным, бисексуальным, трансгендерным и квир-сообществам (ЛГБТК) и иммиграции»[2].

Разновидностями правого экстремизма в данном докладе называют неонацизм, неофашизм и ультранационалистические формирования.

Одним из наиболее известных проявлений неонацизма на Западе является *движение наци-скинхедов*. Скинхеды появились в Англии в конце 60-х гг. XX в. с возникновением движения так называемых «модов» (*mods*), которые были выходцами из бедных рабочих районов английских городов. Они оказались первыми, кто противопоставил свой образ жизни тогдашней английской «золотой молодежи». В 80-е гг. XX в. под влиянием очередной волны переселенцев из Азии и агрессивной социальной политики англий-

[1] Неонацизм // Большая российская энциклопедия. URL: https://bigenc.ru/world_history/text/2260142 (дата обращения: 12.08.2020).

[2] EU Terrorism Situation and Trend report (TE-SAT) 2020 // Europol. 23 June 2020. URL: https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020 (дата обращения: 15.07.2020). Далее — TE-SAT.

ские скинхеды все больше стали превращаться в политизированные боевые группировки расистского толка[1].

Важнейшую роль в формировании движения наци-скинхедов в Великобритании в 1970–1980-х гг. сыграло движение панк-рок-музыки «Рок против коммунизма» (*Rock Against Communism, RAC*). Флагманом движения стала британская рок-группа «Skrewdriver», основанная Яном Стюартом. Группа приобрела культовый статус среди сторонников белого превосходства и до сих пор сохраняет его[2]. Музыкальные записи и концерты «Skrewdriver» и других подобных рок-групп направления «Oi!» стали ключевыми слагаемыми субкультуры «Белой власти» (*White Power*) в Европе.

Скинхеды позиционировали себя как солдат «священной расовой войны», которую ведут люди белой расы против евреев, цыган, негров и прочих «не арийцев», а также наркоманов, гомосексуалистов и левой молодежи. Основу неонацистской идеологии скинхедов составляют идеи расового превосходства. Внешними отличительными чертами скинхедов в полном соответствии с их названием являются бритая голова, а также особый стиль одежды (берцы, джинсы, куртки на молнии, военная униформа) и татуировки с нацистской символикой. Музыкальная компонента субкультуры скинхедов представлена в основном разновидностями панк-рока и тяжелого металла.

В США идеологическую основу концепции белого супрематизма заложили видные деятели данного движения — Джордж Рокуэлл, Уильям Пирс и Дэвид Лэйн. О них стоит сказать немного подробнее, поскольку влияние их идей выходит далеко за национальные границы. Их можно считать вдохновителями всего неонацистского движения на Западе.

Джордж Рокуэлл (George Rockwel) считается отцом американского неонацизма, зародившегося в послевоенные годы. Будучи отставным подполковником вооруженных сил США, он увлекся нацистскими идеями и в 1959 г. основал Американскую нацистскую партию (*American Nazi Party*). Рокуэлл отрицал холокост и старался развивать нацистские идеи в рамках христианской идентичности (напомним, что германская нацистская философия преимущественно апеллировала к языческим культам и мифологии). Именно

---

[1] Движение скинхедов White Power: история создания, идеология. Справка // РИА Новости. 28.10.2008. URL: https://ria.ru/20081028/153936359.html (дата обращения: 12.10.2020).

[2] Skrewdriver // Anti-Defamation League. URL: https://www.adl.org/education/references/hate-symbols/skrewdriver (дата обращения: 28.09.2020).

Рокуэлл изобрел новый девиз-приветствие американских неонацистов — «White Power», вместо прежнего немецкого «Sieg Heil».

Уильям Пирс (William Pierce) также является одним из видных деятелей супрематистского белого движения в США. Его главным вкладом в развитие этого движения стала публикация в 1978 г. романа-антиутопии «Дневники Тёрнера» («Turner Diaries»). В романе Пирса описывается вооруженная борьба белого революционного движения против «системы» (правительства США), находящейся под еврейским контролем и являющейся проводником мультикультурализма. Уничтожение представителей черных рас и евреев, а также предателей белой расы подается как единственный способ решения социальных проблем. «Дневники Тёрнера» считаются главной книгой («библией») среди правых экстремистов США и других стран Запада[1]. Ее особая опасность состоит в том, что она несет идею организации подпольных террористических ячеек и поощряет совершение нападений одиночками. В частности, считается, что она вдохновила действия Тимоти Маквея, совершившего один из крупнейших терактов в истории США — взрыв в федеральном здании в Оклахома-Сити в 1995 г., унесший жизни 168 человек.

Дэвид Лэйн (David Lane) — другая культовая фигура в мировом неонацистском движении — являлся участником нескольких крупных ультраправых группировок в США, включая террористическую организацию «The Order», созданную по образцу революционной структуры, описанной в «Дневниках Тёрнера». Лэйн является автором популярного среди правых радикалов лозунга «14/88», где число «14» означает четырнадцать слов неонацистского идеолога Дэвида Лэйна: «We must secure the existence of our people and a future for White children» («Мы должны защитить само существование нашего народа и будущее для белых детей»), а число 88 является закодированным приветствием «Heil Hitler!» («Хайль Гитлер!»), поскольку буква «H» стоит в латинском алфавите восьмой, и в то же время означает 88 заповедей Дэвида Лэйна.

2. Хронология атак правых экстремистов в странах Запада

В последние два десятилетия правый экстремизм на Западе постепенно набирал силу. С начала 2000-х гг. в европейских странах и иных государствах Западного мира было совершено большое

[1] *Berger J.M.* The Turner Legacy: The Storied Origins and Enduring Impact of White Nationalism's Deadly Bible. ICCT Research Paper September 2016 // The International Centre for Counter-Terrorism. URL: http://icct.nl/app/uploads/2016/09/ICCT-Berger-The-Turner-Legacy-September2016-2.pdf (дата обращения: 14.01.2021).

количество террористических атак и экстремистских нападений. Ниже приведен перечень наиболее крупных из них[1].

9 июня 2004 г. Германия, г. Кельн: подрыв взрывного устройства у парикмахерской, где проживало большое число турецких иммигрантов. Пострадали 22 человека. Организаторы теракта долгое время оставались неизвестными, пока в 2011 г. ответственность за него не взяла на себя правоэкстремистская группировка «Национал-социалистическое подполье», которая организовала еще несколько убийств и нападений в 2000-х — начале 2010-х гг.

22 июля 2011 г., Норвегия, г. Осло и остров Утёйа: двойной теракт, совершенный Андерсом Брейвиком. Сначала преступник взорвал бомбу в столичном правительственном квартале, в результате чего погибли восемь человек. Через несколько часов на острове, где проводится молодежный слет правящей Норвежской рабочей партии, Брейвик устроил стрельбу из карабина и пистолета, убив еще 69 человек. Таким образом, теракт унес жизни 77 человек, при этом свыше 150 человек получили ранения.

13 апреля 2014 г., США, г. Оверленд-Парк (*штат Канзас*): стрельба по людям из дробовика в центре городской еврейской общины и в доме престарелых «Деревня шалом». Погибли три человека, еще двое были ранены. Нападавшим оказался 73-летний Фрейзер Гленн Миллер-младший, член различных американских националистических группировок и «Ку-клус-клана».

17 июня 2015 г., США, г. Чарлстон (*штат Южная Каролина*): стрельба по людям из пистолета в методистской епископальной церкви. В результате погибли девять темнокожих прихожан, в том числе пастор церкви и сенатор законодательного собрания штата. Убийцей оказался 21-летний Дилан Руф, сторонник теории белого превосходства.

12 августа 2017 г., США, г. Шарлотсвилл (*штат Вирджиния*): во время массовых беспорядков в городе автомобиль совершил умышленный наезд на участников протестов (в городе шло длительное противостояние белых националистов и их противников). Один человек погиб, 19 получили ранения. Преступление было совершено 20-летним жителем штата Огайо, неонацистом Джеймсом Алексом Филдсом по мотивам ненависти.

29 января 2017 г., г. Квебек-Сити (*провинция Квебек*), *Канада*: стрельба по прихожанам мечети во время вечерней молитвы. В ре-

[1] При подготовке данного блока использовался материал ТАСС. См.: Случаи терактов, осуществленных правыми радикалами // ТАСС. 2019. 15 мар. URL: https://tass.ru/info/6221324 (дата обращения: 31.08.2020).

зультате нападения шесть человек погибли, 18 получили ранения. Нападавшим оказался канадец праворадикальных взглядов Александр Биссоннетт.

27 октября 2018 г., США, г. Питтсбург (*штат Пенсильвания*): расстрел из винтовки прихожан синагоги «Древо жизни». Погибли 11 человек, шесть человек получили ранения. Нападавшим оказался 46-летний Роберт Бауэрс, действовавший по мотивам ненависти по отношению к евреям.

15 марта 2019 г., Новая Зеландия, г. Крайстчерч: стрельба из автоматического оружия по прихожанам мечетей. Сначала преступник расстрелял людей в мечети Аль-Нур, а затем — посетителей исламского центра Линвуда. Погиб 51 человек, 49 получили ранения. Расстрел произвел гражданин Австралии Брентон Таррант.

27 апреля 2019 г., США, г. Повей (*штат Калифорния*): стрельба из автоматического оружия по прихожанам синагоги. Один человек погиб, трое получили ранения, включая раввина синагоги. Жертв могло быть гораздо больше, если бы у преступника не заклинило оружие. Нападавшим оказался 19-летний местный житель Джон Эрнест, действовавший на почве антисемитизма.

3 августа 2019 г., США, г. Эль-Пасо (*штат Техас*): расстрел из автоматического оружия посетителей торгового центра «Wallmart». Погибли 22 человека, 24 были ранены. Нападавшим оказался 21-летний житель расположенного в 650 милях от Эль-Пасо города Аллен Патрик Вуд Крузиус, сторонник теории «белого геноцида» (см. ниже).

9 октября 2019 г., Германия, г. Галле (*земля Саксония-Анхальт*): 27-летний немец попытался напасть на синагогу, где верующие праздновали еврейский праздник Йом-Кипур. Не сумев открыть запертые входные двери выстрелами и с помощью СВУ, он произвел случайный выстрел и убил женщину, проходившую мимо. Затем он заехал в турецкий ресторан, где убил еще одного мужчину. По пути следования он неоднократно стрелял в других людей, двоих из них серьезно ранив. Преступником оказался 27-летний гражданин Германии Стефан Баллит. Мотивом преступления также выступали антисемитские убеждения.

Данные за 2020 г. пока не опубликованы правоохранительными органами и международными организациями. Вместе с тем в докладе Центра стратегических и международных исследований от октября 2020 г. указано, что белые супрематисты и их единомышленники осуществили 67% террористических заговоров и на-

падений в США в 2020 г.[1] Определенно, наиболее резонансной акцией ультраправых в США последнего времени стал захват Капитолия 6 января 2021 г. Хотя среди разношерстной толпы, принимавшей участие в штурме, было много активистов разных движений, считается, что крайне правые сыграли в захвате ключевую роль[2]. Хотя имеется и альтернативная точка зрения, рассматривающая штурм как умышленную провокацию против Трампа, организованную спецслужбами США с привлечением провокаторов из «Антифа» и BLM[3].

3. Современные идеологические течения правого экстремизма на Западе

Идеологическая база современного правого экстремизма на Западе не являет собой некий монолит. Как справедливо отмечается в докладе TE-SAT 2020, праворадикальная экстремистская идеология неоднородна и имеет множество течений, единых в своем неприятии разнообразия и прав меньшинств. Основными элементами насильственной правой идеологии являются вера в превосходство «белой расы» и представление о том, что насильственные действия отдельных лиц, входящих в состав «безлидерного сопротивления», служат разжиганию «расовой войны». Это противостояние считается неизбежным, оно необходимо для того, чтобы остановить предполагаемый заговор «системы» по замене белого населения путем массовой иммиграции[4].

Как утверждают авторы доклада, спектр правых экстремистов неоднороден в своих проявлениях — это смесь предрассудков, презрительных и тоталитарных идеологий, каждая из которых по-своему представляет угрозу безопасности. К ним относятся: национал-социалистические и неонацистские группы; ревизионисты и ревизионистские группы; расистские и антиеврейские группы; а также скинхеды и праворадикальные экстремистские хулиган-

---

1 The War Comes Home: The Evolution of Domestic Terrorism in the United States. CSIS Briefs October 22, 2020 // Center for Strategic and International Studies. URL: https://www.csis.org/analysis/war-comes-home-evolution-domestic-terrorism-united-states (дата обращения: 27.01.2021).

2 *Makuch B.* Neo-Nazis Boast About Participation In Capitol Hill Invasion // Vice news. Jan 7, 2021. URL: https://www.vice.com/en/article/93wnja/neo-nazis-boast-about-participation-in-capitol-hill-invasion (дата обращения: 27.01.2021).

3 *Овчинский В.* Капкан для Трампа // Завтра. 2021. 7 янв. URL: https://zavtra.ru/blogs/kapkan_dlya_trampa (дата обращения: 08.01.2021).

4 TE-SAT.

ские группы. Кроме того, правый экстремизм опирается на целый ряд других субкультур ненависти, которые отвергают разнообразие и считают религиозные, этнические или сексуальные меньшинства врагами[1].

В докладе TE-SAT 2020 выделены три основных направления правой идеологии[2]:

1. *Культурный национализм* — вера в то, что «западная культура»[3] находится под угрозой воздействия массовой миграции в Европу и отсутствия интеграции со стороны определенных этнических и культурных групп. Культурный национализм, как правило, фокусируется на неприятии некоторых культурных практик, таких как ношение закрывающей лицо вуали (паранджи или никаба), или предполагаемых попыток навязать исламское право в западных странах.

2. *Белый, или этнический национализм*, — вера в то, что массовая миграция из «небелого» мира и предполагаемые демографические изменения представляют экзистенциальную угрозу для «белой расы» и «западной культуры». Белый национализм выступает за создание «белой» родины либо путем разделения уже существующих стран, либо путем репатриации этнических меньшинств (при необходимости принудительной). Бóльшая часть этой риторики присутствует в идентитаристском движении.

3. *Белый супрематизм* — вера в то, что «белая раса» обладает определенными неотъемлемыми физическими и умственными характеристиками, которые обусловливают ее превосходство над другими расами. Хотя далеко не все сторонники идей белого превосходства являются воинствующими, идеология белого превосходства способна более, чем другие формы правого экстремизма, вдохновлять акты серьезного насилия или терроризма. Это связано с явным поощрением данной идеологией ненависти и насилия в отношении меньшинств.

Приведенные направления праворадикальной идеологии разделяются широким спектром националистических организаций

---

1 TE-SAT.

2 Там же.

3 Словосочетание «западная культура», равно как «белая раса» и некоторые другие, приводятся в тексте доклада TE-SAT в кавычках. Это может означать как стремление авторов указать на то, что данные понятия используются в значении, придаваемом им правыми радикалами, так и то, что составители доклада не признают существования описываемых данными понятиями явлений реальности.

и групп. Среди них по-прежнему много неонацистских группировок.

Одна из самых известных групп — «*Кровь и честь*» (*Blood & Honour*, *B&H*), созданная в Великобритании в 1987 г. Ее цель — подготовка «политических солдат» для ведения «расовой войны» и спасения «белой расы». Организация имеет отделения в различных европейских странах, включая Бельгию и Португалию. Она была запрещена в Германии в 2000 г. Бельгия сообщила, что в 2019 г. B&H, которая в прошлом ослабла из-за внутреннего инакомыслия и раскола, занималась в основном сетевой деятельностью, такой как музыкальные концерты, а не активизмом и распространением идеологии.

Продолжает функционировать и другая крупная неонацистская организация «*Нация Хамерскина*» (*Hammerskin Nation*), изначально созданная в 1988 г. в США и считающаяся там одной из самых организованных групп наци-скинхедов. В докладе TE-SAT 2020 отмечается, что несмотря на снижение способности мобилизовать последователей и членов, данная организация организовала ряд крупных мероприятий с участием своих сторонников в Европе, в частности так называемые «Совещания европейских офицеров» (*European Officers Meeting*). Кроме того, в марте группа провела встречу в Лиссабоне, собрав вместе разные поколения скинхедов, включая ветеранов боевых действий из несуществующего ныне «Национального движения действий» (*Movimento de Agao Nacional*, *MAN*) и бывших членов музыкальных рок-групп «Ненависть» (*Odio*) и «Железная гвардия» (*Guarda de Ferro*), которые прекратили свою деятельность несколькими годами ранее.

Среди других сохраняющих свою активность групп неонацистов, в докладе Европола фигурируют: «*Северное движение сопротивления*» (*Nordiska motstandsrorelsen*, *NMR*) — праворадикальное движение, действующее в Финляндии и Швеции, «*Правое сопротивление*» (*Right-Wing Resistance*, *RWR*) — небольшая праворадикальная экстремистская группа с международными связями, действующая в Бельгии и Швеции; греческая ячейка крупной глобальной праворадикальной террористической организации «*Сражение 18*» (*Combat 18*) — «Сражение 18 Эллада» (*Combat 18 Hellas*) и др.

Появлялись и новые группировки неонацистов. В частности, отколовшаяся группа участников «Северного движения сопротивления» (NMR) основала новую организацию «*Нордическая сила*» (*Nordisk Styrka*, *NS*). Они якобы были недовольны парламентской направленностью *NMR*.

В качестве опасной тенденции в докладе Европола отмечена активная военизированная подготовка европейских неонацистов, включающая организацию лагерей для подготовки по стрельбе из огнестрельного оружия, боевым искусствам и обучения навыкам выживания. Ради прохождения такой подготовки они выезжают в другие страны Европы.

Одной из прикладных идеологических концепций современных правых экстремистов на Западе выступает «*безлидерное сопротивление*». Правое террористическое и экстремистское насилие часто преследует цель спровоцировать «расовую войну», которую многие правые экстремисты считают неизбежной. Они добиваются ответной насильственной реакции со стороны жертв насилия и их окружения. Такие инициирующие действия изображаются как часть «безлидерного сопротивления» — концепции, которая направлена на поощрение одиночных субъектов к совершению насилия.

Концепция безлидерного сопротивления была описана в сборнике информационных бюллетеней «Осада» (SIEGE), выпущенных американским неонацистом Джеймсом Мейсоном (James Mason) в 1980-х гг. SIEGE выступает за партизанскую войну небольших автономных ячеек против того, что называется «системой»[1]. Среди действующих групп, пропагандирующих идеи SIEGE, выделяют неонацистские организации, названные «дивизиями», включая «*Дивизию ядерного оружия*» (*Atomwaffen Division*), «*Дивизию солнечной войны*» (*Sonnenkrieger Division*) и «*Дивизию огненной войны*» (*Feuerkrieg Division*). Они действуют в США, Канаде и европейских странах.

В целом в США картина праворадикальных движений во многом схожа с европейской, однако имеет и существенные отличия. На сайте правозащитной организации «Южный правовой центр по вопросам бедности» (*Southern Poverty Law Center, SPLC*) в настоящее время выделено 68 экстремистских групп, большинство из которых относятся к праворадикальному крылу[2].

В аналитической статье «EADaily», посвященной правому крылу внутреннего терроризма в США, к носителям экстремист-

[1] *Ware J.* 'Siege: The Atomwaffen Division and Rising Far-Right Terrorism in the United States', ICCT Policy Brief, 2019 // The International Centre for Counter-Terrorism. URL: https://icct.nl/publication/siege-the-atomwaffen-division-and-rising-far-right-terrorism-in-the-united-states/ (дата обращения: 12.09.2020).

[2] Groups // Southern Poverty Law Center. URL: https://www.splcenter.org/fighting-hate/extremist-files/groups (дата обращения: 22.01.2021).

ских идеологий внутри белого национализма относятся: белые супрематисты и нацисты; скинхеды; антигосударственные активисты; «суверенные граждане»; самопровозглашенная «милиция» — «ополчение»[1]. Хотя упомянутый Южный правовой центр по вопросам бедности использует более дробную классификацию и выделяет 20 разновидностей экстремистских идеологий (альтернативные правые, антииммигрантское движение, анти-исламизм, антиправительственное движение, движение за христианскую идентичность, неонацисты, расистские скинхеды и т.д.)[2].

Кратко рассмотрим некоторые наиболее крупные идеологические течения ультраправых в США.

Белые супрематисты (*White Supremacy*). Термин «белый супрематистский экстремизм» (*white supremacist extremism*, *WSE*) описывает людей или группы, которые совершают преступные действия во имя идеи расового превосходства белых. По сведениям «Foreign Policy», в мае 2017 г. ФБР и Министерство внутренней безопасности США выпустили для служебного пользования совместный бюллетень, в котором утверждалось, что белые супрематисты «несут ответственность за 49 убийств в 26 нападениях с 2000 по 2016 г. — больше, чем любое другое внутреннее экстремистское движение».

Идеология американского супрематизма утверждает, что белая раса стоит выше всех остальных. Именно носители белой расы создали и поддерживают на планете и в США, в частности, цивилизацию. Из-за особенностей демократической культуры США, благодаря 1-й поправке к конституции, «белый супрематистский экстремизм» опирается на конституционно защищенную деятельность широкого круга групп, публично пропагандирующих ненависть, начиная от «Ку-клукс-клана» и заканчивая скинхедами[3].

Антидиффамационная лига выделяет четыре ключевых принципа белого супрематизма: 1) белые должны доминировать над людьми другого происхождения, особенно там, где они могут сосуществовать; 2) белые должны жить сами по себе в обществе, состоящем только из белых; 3) белые люди имеют свою собственную

---

[1] Внутренний терроризм США: супрематисты и другие белые националисты // EADaily. 2017. 14 сент. URL: https://eadaily.com/ru/news/2017/09/14/vnutrenniy-terrorizm-ssha-suprematisty-i-drugie-belye-nacionalisty (дата обращения: 19.09.2020).

[2] Ideologies // Southern Poverty Law Center. URL: https://www.splcenter.org/fighting-hate/extremist-files/ideology (дата обращения: 22.01.2021).

[3] Ibid.

«культуру», которая превосходит другие культуры; 4) белые люди генетически превосходят других людей[1].

Большая часть белых супрематистов США делит мир на белых и все другие народы, которые считаются врагами белых. Особая ненависть направлена на афроамериканцев и евреев. Общий расистский исторический рефрен в отношении последних заключается в том, что движение за гражданские права с 1960-х гг. якобы преуспело только потому, что евреи организовали его за кулисами и далее поддержали. Супрематисты убеждены, что евреи проводят в США либеральный порядок и мультикультурализм для того, чтобы разложить американское общество.

Многие белые супрематисты верят в существование в Вашингтоне (США) «сионистского оккупационного правительства» (*Zionist Occupied Government, ZOG*). Согласно этой концепции федеральное правительство США контролируется и манипулируется в интересах международного еврейства. ZOG, в свою очередь, контролирует в США средства массовой информации, искусство, религию, науку и образование.

Белые супрематисты верят в принцип расового разделения — сегрегацию и полагают, что современное общество дискриминирует белых. Они также считают, что белая раса находится под угрозой вымирания из-за растущего «потока» небелых, которые контролируются и манипулируются евреями, и что неизбежные действия необходимы для «спасения» белой расы.

Антиправительственный активизм в США представлен движениями милиции и суверенных граждан[2].

Движение ополчения (*Militia Movement*) представляет собой антиправительственное экстремистское движение, которое стало заметным с 1990-х гг. (после инцидентов в Руби-Ридж в 1992 г. и Уэйко в 1993 г.). Движение объединяет совокупность вооруженных, военизированных групп, сформированных для предотвращения вмешательства «чуждого правительства», под которым понималось правительство США. Участники движения милиции полагают, что правительство США манипулируется скрытым заговором («новым мировым порядком»). Сторонники ополчения клянутся бороться против этого заговора, обычно сравнивая себя с ко-

[1] White Supremacy // Anti-Defamation League. URL: https://www.adl.org/resources/glossary-terms/white-supremacy (дата обращения: 04.09.2020).

[2] Внутренний терроризм США: супрематисты и другие белые националисты.

лонистами, которые подняли оружие против британцев во время войны за независимость[1].

Идеология милиции выступает против запрета свободного владения оружием, т.е. отмены 2-й поправки к конституции США. Кроме того, движение использует отсылку к норме данной поправки, помимо свободы оружия закрепляющей, что «хорошо организованное ополчение необходимо для обеспечения безопасности свободного государства».

Некоторые приверженцы милиции верят в антисемитские и расистские идеологии и одновременно состоят в супрематистских и нацистских сетях. Группы милиции обычно объединяются вокруг конкретного лидера. «Ополченцы» могут собираться для военно-спортивных тренировок, для совместных упражнений на стрельбищах и отработки навыков выживания. Представители движения милиции были замечены в столкновениях с полицией и уличены в подготовке нескольких терактов.

Движение суверенных граждан представляет собой антиправительственное движение, участники которого провозглашают свою независимость (суверенитет) от США. Они не признают полномочий государственных органов, законов и валюты США. Многие члены движения суверенных граждан считают, что правительство Соединенных Штатов является незаконным. Элементом идеологии «суверенов» является вера в заговор, ZOG и идеи белого супрематизма. «Суверенные граждане» отвергают легитимность большей части правовой системы США. Многие считают, что 14-я поправка к Конституции о предоставлении гражданства неграм увела нацию от ее первоначальных корней всеобщего права и прав государства в сторону «федеральной корпорации», которая юридически поработила всех. Именно 14-я поправка, с их точки зрения, сделала незаконным федеральное правительство, отменив права личности и заменив их системами тотального контроля.

Движение «суверенов» включает в себя несколько организованных групп. Например, «Республика для Соединенных Штатов Америки» (*RuSA*) базируется на штате Алабама. Последователи движения также были отмечены в столкновениях с полицией.

В последние годы в США получили развитие несколько белых праворадикальных вооруженных движений, которые противостоят движениям левого толка «Antifa» и «Black Lives Matter». Наиболее видными среди них являются *Boogaloo Movement* и *Proud Boys*. Дви-

[1] Militia Movement // Anti-Defamation League. URL: https://www.adl.org/resources/glossary-terms/militia-movement (дата обращения: 04.09.2020).

жение «Бугалу» носит преимущественно антиправительственный характер и активно проявляет себя участием в различных митингах и шествиях, равно как и в онлайне[1]. «Гордые парни» (*Proud Boys*) являются более четко выраженными сторонниками белого супрематизма и исповедуют исламофобские, антииммигрантские и женоненавистнические идеи[2]. Оба движения придают особое значение защите конституционного права на владение оружием, хотя в большей степени это значимо для «Бугалу»[3].

Кроме того, современным правым экстремистам в США и иных странах Запада свойственны антифеминистские и женоненавистнические взгляды[4]. В частности, их придерживался новозеландский стрелок Таррант. Такие идеи обеспечивают рационализацию сексуальной фрустрации. В сети существует целая сеть блогов и форумов, продвигающих идеи ненависти к женщинам (мизогинии) и защиты прав мужчин, именуемых «маносферой» (*manosphere*)[5]. Феминизм в таких сообществах трактуется как инструмент осуществления белого геноцида. Наиболее ярким радикальным проявлением течения мизогинии выступает движение «*Вынужденное воздержание*» или *InCel* (*involuntary celibate* (*incel*) *movement*). Это женоненавистническое сообщество в основном молодых мужчин встречается в онлайн-пространствах, подобных тем, которые часто посещают белые сторонники превосходства. Данное движение объясняет их неспособность найти сексуальных партнеров тем, что женщины подверглись растлевающему воздействию феминизма и сами свободно выбирают себе мужчин, ориентируясь в основном на их внешность. Обладатели же некрасивой внешности, по мнению инцелов, обречены на длительное отсутствие интимной близости. Движение пропагандирует идею отмщения женщинам за причиненные ими

[1] The Boogaloo Movement // Anti-Defamation League. URL: https://www.adl.org/boogaloo (дата обращения: 27.01.2021).

[2] Ibid.

[3] Boogaloo Boys: вооруженные до зубов американские сторонники неонацизма // Большая война. 27.12.2020. URL: https://big-war.ru/boogaloo-boys-vooruzhennye-do-zubov-amerikanskie-storonniki-neonaczizma/ (дата обращения: 27.01.2021).

[4] When Women are the Enemy: The Intersection of Misogyny and White Supremacy // ADL's Center on Extremism, 2018. URL: https://www.adl.org/media/11707/download (дата обращения: 15.01.2021).

[5] *Basu T.* The "manosphere" is getting more toxic as angry men join the incels // MIT Technology Review. February 7, 2020. URL: https://www.technologyreview.com/2020/02/07/349052/the-manosphere-is-getting-more-toxic-as-angry-men-join-the-incels/ (дата обращения: 15.01.2021).

страдания[1]. В движении есть свой культовый «герой» — Эллиот Роджер, который, реализуя идею мести женскому полу, убил шесть и ранил свыше 10 человек в Айла-Висте в Калифорнии, а затем совершил самоубийство[2]. Впоследствии было совершено несколько подражательных нападений такого рода в США.

В последнее время обширная конспирология, составляющая солидную часть идеологического базиса современного западного неонацизма, пополняется весьма причудливыми теориями. Среди них можно выделить, в частности, теорию заговора «*КАнон*» (*QAnon*), которая изначально возникла в США в 2017 г. после серии постов загадочного пользователя под ником «Q» на популярном сетевом имиджборде 4Chan. Данная конспирологическая теория, а точнее их комплекс, говорит о существовании в глобальной теневой клике лиц, которые занимаются сексуальной эксплуатацией детей и поклоняются сатане. Эта теневая элитная группа, именуемая «глубинным государством» (*The Deep State*) или «заговорщиками» (*The Cabal*), контролирует правительства стран мира. Теория утверждает, что почти каждый президент в новейшей американской истории вплоть до Дональда Трампа был марионеткой, поставленной на свое место глобальной элитой властных брокеров, одержимых обогащением и поддержанием своего сатанинского сексуального культа, убивающего детей. Последователи «QAnon» считают, что эта теневая клика включает в себя ведущих демократов, включая Хиллари Клинтон, Барака Обаму и Джорджа Сороса, а также ряд артистов и голливудских знаменитостей, таких как Опра Уинфри, Том Хэнкс, Эллен Дедженерес, и религиозных деятелей, включая Папу Франциска и Далай-ламу. Впоследствии теория стала обрастать все новыми деталями, однако ее основу составляет представление о некоем глобальном заговоре клики педофилов, который пытается разоблачить Дональд Трамп[3].

Как отмечается в справке Антидиффамационной лиги, несмотря на полное отсутствие каких-либо подтверждающих доказательств,

---

1 *Hale L.* Инцелы. Как кучка девственников превратилась в радикальное движение // Сплетник. 2018. 19 дек. URL: https://spletnik.ru/blogs/govoryat_chto/164677_intcely-kak-kuchka-devstvennikov-prevratilas-v-radikalnoe-dvizhenie (дата обращения: 02.01.2021).

2 Elliot Rodger: How misogynist killer became “incel hero”, 26 April 2018 // BBC News. URL: https://www.bbc.com/news/world-uscanada-43892189 (дата обращения: 02.01.2021).

3 *Roose K.* What Is QAnon, the Viral Pro-Trump Conspiracy Theory // NY Times. Sept. 1, 2020. URL: https://www.nytimes.com/article/what-is-qanon.html (дата обращения: 15.09.2020).

«QAnon» успешно «совершил прыжок из параноидальных катакомб онлайн-субкультуры в основное консервативное движение Америки»[1]. При этом подчеркивается, что хотя приверженцы «QAnon» не являются экстремистами, эта опасная теория вдохновляла насильственные действия. Не случайно, в докладе ФБР от мая 2019 г., «QAnon» наряду с другими теориями заговора, мотивирующими своих последователей к совершению преступлений, был отмечен как новая угроза внутреннего терроризма[2].

Движение контрджихада: новое поколение правых радикалов в Европе и США. После серии терактов в западных странах в 2000-е гг., включая серию терактов 11 сентября 2001 г. в США и взрывы в Лондоне 7 июля 2005 г., получает развитие *движение контрджихада* (*Counter-jihad movement*), которое обозначает ислам и мусульман как экзистенциальную угрозу для Западной цивилизации. Движение возникает стихийно и включает в себя неструктурированную сеть мыслителей, блогеров, активистов, аналитических центров, уличных движений и групп по обе стороны Атлантики. В Европе сторонники движения в основном сосредоточены на проблеме стремительной исламизации европейских стран, которой не в силах противостоять недееспособная европейская бюрократия.

В начале 2000-х британской писательницей Бат Йеор (Bat Ye'or), также известной как Жизель Литтман (Gisèle Littman), была сформулирована концепция «Еврабии», согласно которой европейские страны постепенно покоряются исламу и переходят под исламское правление[3]. По мнению сторонников концепции, Европа оказывается в состоянии, в котором она вынуждена отрицать свою собственную культуру, молча наблюдать мусульманские зверства, принимать мусульманскую иммиграцию и платить дань через различные виды экономической помощи.

Данный нарратив приобрел важное значение для выражения антиисламских настроений и был использован исламофобскими движениями, в частности таким, как «Остановить исламизацию Европы» (*Stop Islamisation of Europe*, *SIOE*), образованным в 2007 г. в результате слияние антиисламских групп датских и английских

---

1 QAnon // Anti-Defamation League. URL: https://www.adl.org/qanon?fbclid=IwAR02jP48O9FRvPOy_OZSafkqhmvKGiL9XRbc5tKxxppqfBWbydUjR8RtyYY (дата обращения: 04.09.2020).

2 *Winter J.* Exclusive: FBI document warns conspiracy theories are a new domestic terrorism threat // Yahoo News. Aug 1, 2019. URL: https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html (дата обращения: 04.09.2020).

3 Eurabia: The Euro-Arab Axis. Fairleigh Dickinson University Press, 2005.

активистов. Известно, что норвежский террорист Андерс Брейвик активно ссылался на Еврабию как концепцию исламизации[1].

После серии крупных терактов в западных странах, спланированных или инспирированных «Исламским государством», в 2014-м и последующие годы в них начали стихийно формироваться «отряды самообороны» для «борьбы с исламской угрозой» в рамках движения контрджихада. Например, во Франции были образованы патриотические группы самообороны, которые черпают вдохновение из организационных моделей военизированных структур и (или) участников движений за выживание. В Бельгии правые экстремистские группы неоднократно организовывали патрули самообороны в общественных местах, якобы для того, чтобы обезопасить жителей от «агрессии, совершаемой мигрантами», под предлогом неспособности государства обеспечить надлежащую безопасность. В Словении стали создавать «соседские дозоры», мотивируя это тем, что нынешние государственные меры не обеспечивают достаточный уровень безопасности граждан от мигрантов. Эти движения и группы вербуют своих членов через социальные сети. Группы имеют единое командование, преследуют схожие цели, проводят обучение армейской технике, имеют единые знаки отличия и проводят разъяснительную работу с общественностью и конкретными целевыми группами[2].

Вместе с тем антииммигрантские и исламофобские настроения стали основой для формирования и более умеренного политического представительства правых сил, которые в Европе обычно обозначают как *движение «Новых правых»* (*англ. New Right*, *фр. Nouvelle Droite*). Ключевые темы этих правых активистов — антииммиграция, анти-мультикультурализм, неприятие ислама и осознание бессилия политического истеблишмента. Они утверждают, что западная культура должна быть очищена от мусульманской иммиграции и «исламизации». В своей пропаганде новые правые используют социальные вопросы, например, проводя сравнение условий жизни мигрантов и бедственного положения бездомных[3]. Идейную основу движения европейских новых правых (*European New Right*) заложили в 1960-е гг. французские интеллектуалы, объединенные «мозговым» центром GRECE (*Groupement de recherche*

[1] *Fekete L.* The Muslim conspiracy theory and the Oslo massacre // Race & Class. 2011. Vol. 53 (3). Dec. URL: https://journals.sagepub.com/doi/abs/10.1177/0306396811425984? journalCode=racb (дата обращения: 15.07.2020).

[2] TE-SAT.

[3] Там же.

et d'études pour la civilisation européenne, «Группа изучения Европейской цивилизации»). Одним из наиболее видных ее представителей выступал философ Ален де Бенуа (Alain de Benoist)[1].

В настоящее время новые правые представлены широким спектром политических партий, таких как немецкая «Альтернатива для Германии» (*Alternative für Deutschland*, *AfD*), «Австрийская партия свободы» (*Freiheitliche Partei Österreichs*, *FPÖ*), французский «Национальный фронт» (*Front National*), итальянская «Северная лига» (*Lega Nord*), испанская партия «Голос» (*VOX*) и др.[2] Эти политические движения разделяют идеологическую предпосылку надвигающегося «вторжения на Запад»[3].

В США новое поколение движения белых националистов называют «альтернативно правыми» (*Alternative right*) или сокращенно «альт-правыми» (*Alt-right*). Широкое распространение термин получил благодаря Ричарду Спенсеру (Richard Spencer), президенту «Института национальной политики» (*National Policy Institute*) и одному из наиболее известных представителей движения. Зонтичный бренд альтернативно правых объединяет разрозненную совокупность сторонников идей белого супрематизма, расизма, национализма, антисемитизма и антиисламизма. Многие из его сторонников сознательно дистанцируются от неонацизма и фашизма и стремятся придать движению респектабельности, хотя другие, известные как «сцена 1488», открыто проповедуют правые экстремистские идеи. Движение известно своей онлайн-мобилизацией и использованием интернет-культуры в своих коммуникациях, в частности интернет-мемов. Альт-правые активно поддерживали Дональда Трампа на выборах президента США в 2016 г. и в последующий период, а потому тяжело восприняли то, что он уступил Джозефу Байдену в ходе избирательной кампании 2020 г. Движение также активно проявило себя в ходе крупной политической акции в Шарлотсвилле под названием «марш объединенных правых» (*Unite the Right rally*), который закончился массовыми беспорядками и насилием.

Наиболее радикальное крыло правого движения в странах Западного мира обычно обозначается как «*крайне правые*» (*far-*

---

[1] *Бенуа А. де.* Против либерализма: к четвертой политической теории: пер. с фр.; предисл. А. Дугина. СПб.: Амфора, 2009.

[2] См. подробнее: *Бышок С.* Брекзит и евроскептики. Европейцы против ЕС. М.: Книжный мир, 2016.

[3] *Ebner J.* Who are Europe's far-right identitarians? // POLITICO. 04.04.19. URL: https://www.politico.eu/article/who-are-europe-far-right-identitarians-austria-generation-identity-martin-sellner/ (дата обращения: 22.09.2020).

right). Данный термин также имеет аналог — «ультраправые». Хотя грань между новыми (альт-) и крайне правыми зачастую весьма тонка и подвижна. В середине 2010-х гг. наиболее известным ультраправым политическим движением в Европе стала «*Пегида*» (*Pegida*). Данная аббревиатура расшифровывается как «Патриотически настроенные европейцы против исламизации Запада» (нем. *Patriotische Europäer gegen die Islamisierung des Abendlandes*). Изначально возникнув в Германии в 2014 г., движение приобрело характер пан-европейского. «Пегида» выступает за сохранение христианской культуры и против исламистского экстремизма. Она резко критиковала власти за проводимую иммиграционную политику.

В настоящий момент наиболее заметной ультраправой организацией в Европе является «*Идентитаристское движение*» (*Identitarian Movement*). Участники движения выступают за сегрегацию по этническим признакам и утверждают, что «белые» жители Запада имеют право защищать «свои» нации от иностранных народов и культур[1]. Идентитаристы выступают за «реэмиграцию», под которой, по мнению экспертов, понимается массовая депортация всех европейских жителей с мигрантским происхождением или небелой кожей[2].

Европол говорит о данном движении в контексте экстремизма. В частности, отмечается, что «Идентитаристское движение Австрии» (*Identitare Bewegung Osterreichs*, *IBO*) зарекомендовало себя как наиболее активная праворадикальная экстремистская группировка. У нее есть харизматический лидер — Мартин Зельнер (Martin Sellner), являющийся одним из наиболее видных европейских активистов идентитаристского движения. Вместе со своими «братскими» организациями в Европе, IBO в первую очередь способствует сопротивлению воспринимаемой «исламизации» западного мира. В Португалии одной из наиболее активных групп идентичности является «Щит идентичности» (*Escudo Identitario*). По оценкам Португалии, деятельность неонацистских групп тесно связана с группами и организациями европейского идентитаристского движения.

---

1 *Bjørgo T., Ravndal J.A.* Extreme-right violence and terrorism: concepts, patterns, and responses // ICCT Policy Brief, 23 Sept 2019. URL: https://icct.nl/publication/extreme-right-violence-and-terrorism-concepts-patterns-and-responses (дата обращения: 15.07.2020).

2 *Ebner J.* Who are Europe's far-right identitarians? // POLITICO. 04.04.19. URL: https://www.politico.eu/article/who-are-europe-far-right-identitarians-austria-generation-identity-martin-sellner/ (дата обращения: 22.09.2020).

Особо следует отметить идеологическую основу Идентитаристского движения, которую составляет так называемая «теория великого замещения». По мнению исследователей из Института стратегического диалога (*Institute for Strategic Dialogue*) данная теория стала идейным мейнстримом правового радикализма в Европе и получила широкую поддержку среди европейских правых политиков[1]. Именно такое название (*Great Replacement*) было вынесено на обложку манифеста новозеландского террориста Брента Тарранта. После терактов в Крайстчерче экспоненциальный рост упоминаний о «великом замещении» в социальных сетях привлек к этому термину всеобщее внимание.

В связи с особой значимостью данной концепции в контексте темы нашего исследования рассмотрим ее подробнее.

Теория великого замещения: происхождение и содержание. Теория великого замещения говорит о стремлении глобальной элиты («мирового правительства») заместить «белое» население западных стран на этническом и культурном уровне «небелыми» людьми посредством массовой иммиграции. Данная теория вполне укладывается в более старую концепцию «белого геноцида» (*White Genocide*), которая утверждает, что белая раса умирает «из-за роста небелого населения и принудительной ассимиляции» — процессов, спланированных и направляемых еврейским заговором с целью уничтожения белой расы[2]. В качестве выхода из сложившейся ситуации предлагается реэмиграция (*Remigration*) — принудительная депортация мигрантских общин с целью создания этнически или культурно однородного общества. По мнению экспертов, по сути, реэмиграция означает ненасильственную форму этнической чистки[3].

Теория великого замещения берет свое начало от одноименной книги «Le Grand Remplacement» (2011 г.) французского писателя и общественного деятеля Рено Камю. Он описал, что происходит замещение коренных народов Европы совершенно чуждыми ей

---

1 *Davey J., Ebner J.* “The Great Replacement”: the violent consequences of mainstreamed extremism // Institute for Strategic Dialogue. 2019. URL: https://www.isdglobal.org/isd-publications/the-great-replacement-the-violent-consequences-of-mainstreamed-extremism (дата обращения: 05.09.2020).

2 “White Genocide” // Anti-Defamation League. URL: https://www.adl.org/resources/glossary-terms/white-genocide (дата обращения: 04.09.2020).

3 *Davey J., Ebner J.* “The Great Replacement”: the violent consequences of mainstreamed extremism’. “White Genocide” // Anti-Defamation League. URL: https://www.adl.org/resources/glossary-terms/white-genocide (дата обращения: 15.12.2020).

народами и что это фактически следует назвать нашествием, колонизацией, вытеснением[1]. Идеи Камю во многом созвучны мыслям, озвученным в 1968 г. британским парламентарием Энохом Пауэллом (Enoch Powell) в его знаменитой речи «Реки крови» («Rivers of Blood»)[2], а также изложенным в романе французского писателя Жана Распая (Jean Raspail) «Лагерь святош» («Le Camp des saints») 1973 г.[3] Камю свел их в единую концепцию и придумал ей звучное наименование.

В своей книге Камю так описывает суть процесса «великого замещения»: «Что такое Великое Замещение? Простой факт, что на определенной территории жил народ, обыкновенный народ, хорошо утрясенный веками, объединенный чувством принадлежности к этой земле, к своей культуре, своей манере жить и долгой совместно прожитой истории... И вдруг, почти за одно поколение, на той же территории оказываются два народа, а может, и больше, и они делят между собой эту территорию, более или менее мирно, точнее, совсем уже не мирно»[4]. Писатель подчеркивал эпохальное значение происходящих событий: «Великое Замещение — это смена народа, которая стала возможной благодаря Великой Декультурации — это самый значительный феномен французской истории за последние века, а может быть, и за всю историю Франции... То, что происходит на наших глазах — колонизация Севера Югом — не идет ни в какое сравнение с той колонизацией Юга Севером. Это демографическая колонизация, она неминуемо приведет к концу нашей цивилизации»[5].

После публикации книги во Франции поднялась волна критики с обвинениями автора в нагнетании исламофобии, разжигании ненависти и конспирологии. Эта критика еще более усилилась после теракта в Новой Зеландии и опубликования его исполнителем своего манифеста. Но Камю подчеркивал, что просто описывает реальность: «Великое Замещение — это не теория, это всего лишь

---

1 *Дюбуа Э.* Великое замещение // Журнал Фицрой. 2019. 27 нояб. URL: https://fitzroymag.com/politika/velikoe-zameshhenie/ (дата обращения: 07.09.2020).

2 Энох Пауэлл и «Реки крови» // Liberty & Reason. 20 апреля 2018 г. URL: http://nordickraft.blogspot.com/2018/04/blog-post_20.html (дата обращения: 22.10.2020).

3 *Raspail J.* Le Camp des Saints. Paris, 1973.

4 *Дюбуа Э.* Великое замещение // Журнал Фицрой. 2019. 27 нояб. URL: https://fitzroymag.com/politika/velikoe-zameshhenie/ (дата обращения: 07.09.2020).

5 Там же.

синтагма, это простое обозначение, как Столетняя война, как Французская революция, это обозначение современного исторического периода и самого значительного его феномена. Можно назвать этот феномен другими словами, можно подобрать массу синонимов: массовая иммиграция, миграционный потоп, смена народа и цивилизации, исламизация, африканизация...»[1]

Рено Камю всячески дистанцировался от нападений и терактов, совершаемых под воздействием его концепции, и выступал с их осуждением. Однако использование им сильных выражений, таких как «колонизация», «вторжение» и «оккупация», а также призывы писателя к сопротивлению процессу «великого замещения» трактовались его противниками как завуалированные призывы к насилию. Так, новозеландский стрелок Брентон Таррант называл совершенный им теракт «партизанской диверсией против сил оккупанта»[2]. В январе 2020 г. издание «Summit News» сообщило, что Камю был осужден за публичное подстрекательство к ненависти или насилию на почве происхождения, этнической принадлежности, национальности, расы или религии в своем выступлении в ноябре 2017 г. и был приговорен к двум месяцам условного осуждения[3].

Сила общественного влияния теории великого замещения, на наш взгляд, обусловлена прежде всего тем, что она во многом описывает реально происходящие в странах Европы демографические процессы увеличения количества мигрантов, являющихся носителями иных культурных ценностей и поведенческих установок. Определенная часть из них отказались ассимилироваться и, напротив, стали насаждать свой образ жизни. Многие мигранты оказались вовлеченными в преступную деятельность, включая торговлю наркотиками, сексуальную эксплуатацию и разбойные нападения. Кроме того, в 2010-е гг. по странам Европы прокатилась волна джихадистских терактов, исполнителями которых выступали чаще всего мигранты или дети мигрантов, родившиеся уже

[1] *Дюбуа Э.* Великое замещение // Журнал Фицрой. 2019. 27 нояб. URL: https://fitzroymag.com/politika/velikoe-zameshhenie/ (дата обращения: 07.09.2020).

[2] Готовят теракты? Чем опасны неонацисты // Газета.ру. 07.07.2019. URL: https://www.gazeta.ru/science/2019/07/07_a_12483853.shtml (дата обращения: 08.09.2020).

[3] *Watson P.J.* French Intellectual Sentenced to 2 Months in Prison For Calling Mass Immigration an “Invasion” // Summit News. 21 Jan 2020. URL: https://summit.news/2020/01/21/french-intellectual-sentenced-to-2-months-in-prison-for-calling-mass-immigration-an-invasion/ (дата обращения: 05.12.2020).

в странах проживания. Террористические нападения усилили осознание иммигрантов как экзистенциальной угрозы.

Однако это не отменяет того очевидного факта, что европейский миграционный кризис 2015 г., помимо комплекса объективных причин, был в значительной мере спровоцирован политикой ряда европейских стран, прежде всего Германии[1]. Видный российский историк А. Фурсов указывает на то, что так называемый «миграционный кризис», по мнению ряда экспертов, «в значительно большей степени похож на хорошо спланированную и подготовленную сетевую военно-политическую операцию... Цель данной операции — создание управляемого хаоса; средство — организация широкомасштабных, невиданных со времен Второй мировой войны потоков беженцев и нелегальных мигрантов»[2].

Достоверность таких экспертных оценок сложно оценить, хотя косвенные доказательства этого имеются. Так, считается установленным факт публикации в 2000 г. отделом народонаселения департамента по экономическим и социальным вопросам Организации Объединенных Наций доклада «Замещающая миграция: является ли это решением для сокращающегося и стареющего населения?»[3]. В этом докладе рассматриваются различные сценарии развития демографической ситуации в странах Западного мира и обосновывается решение о необходимости использования иммиграции в качестве инструмента для восполнения сокращающейся рабочей силы: «Замещающая миграция означает международную миграцию, которая необходима стране для компенсации сокращения численности населения и старения населения в результате низкого уровня рождаемости и смертности»[4]. Многие ев-

---

1 «Макс и Мохаммед — все равны» // Лента.ру. 2019. 21 сент. URL: https://lenta.ru/articles/2019/09/21/refugees_welcome/ (дата обращения: 08.09.2020); Меркель признала ошибки Берлина в миграционной политике // РБК. 2018. 17 нояб. URL: https://www.rbc.ru/politics/17/11/2018/5befc99e9a79474026447c03; *Фурсов А.* Ангел смерти // Завтра. 2018. 15 июня. URL: https://zavtra.ru/blogs/angel_smerti (дата обращения: 12.06.2020).

2 *Фурсов А.* Ангел смерти // Завтра. 2018. 15 июня. URL: https://zavtra.ru/blogs/angel_smerti (дата обращения: 12.06.2020).

3 LA DIVISION DE LA POPULATION DES NATIONS UNIES PUBLIE UN RAPPORT SUR LES MIGRATIONS DE REMPLACEMENT. Nations Unies. Communiqué de Presse POP/713, 20 MARS 2000.

4 Cédric Mathiot. L'ONU envisage-t-elle une «migration de remplacement» en France comme le dit Guillaume Larrivé? // Libération. 28 août 2019. URL: https://www.liberation.fr/checknews/2019/08/28/l-onu-envisage-t-elle-une-migration-de-remplacement-en-france-comme-le-dit-guillaume-larrive_1747704 (дата обращения: 07.09.2020).

ропейские политики и ведущие СМИ, однако, говорят о том, что данный доклад носил «скорее теоретический характер» и не выступал руководством к действию.

Тем не менее граждане европейских стран, несомненно, винят в сложившимся кризисе свои правительства, и в этом есть доля истины. Усугубляет ситуацию то, что дав «зеленый свет» огромным потокам мигрантов и породив недовольство коренных жителей, правящие элиты государств Европы начали его всячески подавлять, зажимая его в тиски фальшивой политкорректности и «толерантности». Тем самым выплески недовольства широких масс были канализированы в маргинальные и радикальные формы выражения, включая акты насилия и террористические атаки.

Важным фактором популяризации теории великого замещения стала ее активная пропаганда в интернете. Ученые из Института стратегического диалога (*ISD*) провели исследование и установили постоянное увеличение упоминания теории в основных социальных сетях и мессенджерах. Например, за период с апреля 2012 г. по апрель 2019 г. они выявили около 1,5 млн твитов, ссылающихся на теорию великого замещения, на английском, французском и немецком языках. Количество твитов неуклонно росло в течение семи лет, предшествовавших нападению на Крайстчерч, а количество твитов, упоминающих эту теорию, почти утроилось за четыре года — с чуть более чем 120 тыс. в 2014 г. до немногим более 330 тыс. в 2018 г. Несмотря на доминирование французских аккаунтов в онлайн-обсуждениях теории великого замещения, она становится все более распространенной и на международном уровне[1].

Исследователи установили, что помимо крупных интернет-платформ, теория активно распространялась через альтернативные медиа правого толка (например, французские интернет-сайты *Riposte Laïque* и *Résistance Républicaine*), имиджборды (такие как 8chan и 4chan) и ультра-либертарианские социальные сети (такие, как *Gab* и *Minds*), а также через каналы и чаты в мессенджерах (прежде всего *Telegram*, *Discord*, *WhatsApp*). Сильный импульс широкой популяризации теории придало ее активное использование видными правыми политическими деятелями Европы, такими как премьер-министр Венгрии Виктор Орбан и бывший вице-канцлер Австрии Х.К. Штрахе[2].

[1] *Davey J., Ebner J.* 'The Great Replacement": the violent consequences of mainstreamed extremism.

[2] Ibid.

Авторы исследования из *ISD* подчеркивают общественную опасность теории великого замещения, становящейся мейнстримом европейских праворадикалов: «Теория великого замещения способна вдохновлять своих приверженцев на радикальные действия, начиная от ненасильственных этнических чисток и заканчивая “реэмиграцией” и геноцидом»[1].

Во многом соглашаясь с учеными, отметим следующее. По нашему мнению, теория великого замещения, не содержащая прямых призывов к насилию, способна это насилие порождать, включая совершение жестоких террористических актов, подобно атаке в Крайстчерче. Но вполне очевидно и то, что ее социальный базис ввиду продолжения процессов изменения состава народонаселения стран Европы и связанных с этим проблем будет и дальше расширяться, даже несмотря на отдельные теракты.

4. Пропаганда правого экстремизма и виртуальная экосистема ультраправых

Как и многие другие современные экстремисты, праворадикалы ведут активную пропаганду своей идеологии. Пропагандистские кампании позволяют крайне правым привлечь широкое внимание средств массовой информации и интернет-ресурсов. За счет потока пропаганды экстремисты пытаются сделать привычными свои сообщения и активизировать вербовку новых членов, одновременно нацеливаясь на группы меньшинств, включая евреев, негров, мусульман, небелых иммигрантов и ЛГБТК-сообщество[2].

Правые экстремисты имеют обширный и длительный опыт ведения пропаганды как в офлайне, так и в онлайне. Причем даже в современную цифровую эпоху они по-прежнему уделяют важное значение традиционным для них формам идеологической деятельности, таким как демонстрации и публичные мероприятия, музыкальные концерты, расистские граффити, осквернение религиозных объектов, словесные нападки и другие формы разжигания ненависти. Но современная цифровая среда открыла для них новые уникальные возможности, которыми праворадикалы успешно воспользовались. Этому также благоприятствовало длительное нахождение в тени ИГИЛ и других джихадистских группировок,

[1] *Davey J., Ebner J.* ‘The Great Replacement”: the violent consequences of mainstreamed extremism.

[2] *Weimann G., Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace // International Institute for Counter-Terrorism. 05.04.2020. URL: https://www.ict.org.il/Article/2528/The_Virus_of_Hate#gsc.tab=0 (дата обращения: 12.06.2020).

которым уделялось основное внимание со стороны правоохранительных органов и администрации социальных сетей. Хотя в последнее время ситуация начала кардинально меняться.

Однако вернемся к рассмотрению основных направлений и форм праворадикальной пропаганды.

Пропаганда в офлайне. Крайне правые активисты и их сторонники давно используют пропаганду в качестве инструмента для распространения своих сообщений. Задолго до появления интернета они распространяли экстремистские листовки или ездили из города в город, по пути оставляя свои разжигающие ненависть статьи, брошюры и манифесты. Эти методы все еще используются: например, в 2019 г. сторонники теории белого превосходства в США изготовили небывалый объем печатных материалов для отдельных районов и студенческих городков, в том числе беспрецедентное количество листовок, баннеров, наклеек и плакатов, распространявшихся по всей стране[1].

Как мы отмечали выше, важным фактором популяризации неонацизма в Европе в 1970–1980-е гг. стало движение панк-рок-музыки «Рок против коммунизма» (*Rock Against Communism, RAC*). Концерты «Skrewdriver» и подобных ей рок-групп выступали местом сбора скинхедов и иных ультраправых, внося весомый вклад в трансляцию их идеологии в молодежную среду и формирование соответствующей субкультуры. Для продвижения музыкальных записей и концертов подобных рок-групп лидером «Skrewdriver» Я. Стюартом в 1987 г. была учреждена промоутерская сеть «Кровь и честь» (*Blood & Honour, B&H*), которая существует до сих пор. Неонацистский панк-рок и блэк-метал транслируют послания ненависти, содержат призывы или подстрекательство к насилию, а также прославляют «героев» сторонников белого превосходства[2].

Музыка и концерты продолжают и сейчас играть ключевую роль в символическом обеспечении согласованности действий и распространении неонацистских групп. Некоторые крупные организации неонацистов, такие как американская группировка «Hammerskins», имеют собственные звукозаписывающие лейблы. В последние годы музыка «White Power» активно распространяется через интернет. Однако музыкальные концерты продолжают активно собирать неонацистов в Европе и США. Так, в Португалии каждый год, начиная с 2015 г., местное отделение B&H проводило концерты в начале но-

[1] TE-SAT.

[2] The Sounds of Hate. The White Power Music Scene in the United States // Anti-Defamation League. URL: https://www.adl.org/resources/reports/the-sounds-of-hate (дата обращения: 28.09.2020).

ября. На этих концертах обычно присутствовали известные представители других групп B&H в Европе. Правые экстремистские группы пытаются обойти запреты в одной стране, организуя или посещая собрания/концерты в других странах[1].

К другим офлайновым формам распространения праворадикальной идеологии относятся митинги, шествия и иные публичные акции, которые обычно проводятся в ознаменование годовщин исторических событий. Например, сообщалось, что неонацисты из разных частей Европы собираются каждый февраль в Будапеште, чтобы отметить так называемый «День чести» (*Day of Honour*)[2]. Резонансными публичными акциями характеризуется Идентитаристское движение. Так, немецкое отделение (*Identitäre Bewegung*) привлекло к себе широкое внимание общественности и СМИ дерзкой акцией в 2016 г. в Берлине, где активисты движения взобрались на Бранденбургские ворота и развернули на них транспаранты с лозунгами против беженцев[3].

В европейских странах в качестве опасной тенденции отмечается возрастание интереса правых экстремистов к военизированной подготовке. Их группы регулярно организуют лагеря и полевые выходы, на которых отрабатываются навыки выживания, рукопашного боя и обращения с огнестрельным оружием. Нередко в таких сборах участвуют спортивные ультрас-группировки[4].

Важное значение по-прежнему имеют специфическая символика и атрибутика. Правые экстремисты используют бренды (коммерческие) и символику, чтобы сигнализировать друг другу о приверженности движению. Например, некоторые группы утверждают, что имеют отношение к скандинавской языческой мифологии и используют ее в качестве маркера идентичности (названия групп, гербы, татуировки, куртки и т.д.). Сетевые онлайн-коммуникации повлияли на изменения в темпах и масштабах использования праворадикальной экстремистской символики. Виртуальные группы могут также заниматься коллекционированием нацистской атри-

---

1 TE-SAT.

2 Там же.

3 «Identitäre Bewegung» klettert auf das Brandenburger Tor // Welt. 27.08.2016. URL: https://www.welt.de/politik/deutschland/article157876725/Identitaere-Bewegung-klettert-auf-das-Brandenburger-Tor.html (дата обращения: 21.01.2021); *Хилле П., Жолквер Н.* Германское «Движение за идентичность»: волки в овечьей шкуре // Deutsche Welle. 29.08.2019. URL: https://www.dw.com/ru/германское-движение-за-идентичность-волки-в-овечьей-шкуре/a-50181560 (дата обращения: 21.01.2021).

4 TE-SAT.

бутики в реальной жизни. Так, в ходе проведенного итальянскими «силовиками» обыска в ноябре 2019 г. у последователей неонацистского и антиеврейского движения «Римский арианский орден» (*Ordine Ario Romano*) было изъято большое количество нацистской атрибутики и символики организации «Поколение идентичности» (*Generation Identity*), являющейся ветвью Идентитаристского движения[1].

Онлайн-пропаганда. Правые экстремисты давно присутствуют в интернете и занимают «старые» и «новые» онлайн-пространства, формируя тем самым продвинутую онлайн-экосистему. Развитие продолжалось в течение трех десятилетий с использованием систем досок объявлений, веб-сайтов, онлайн-форумов и в последнее время — социальных сетей. В настоящее время правоэкстремистская интернет-сцена не ограничивается одним типом онлайн-пространства, а представляет собой лоскутное одеяло из различных типов платформ и пространств, на котором хорошо известные платформы социальных сетей являются лишь одним из компонентов. Крайне правые экстремисты генерируют контент на различных онлайн-платформах и все чаще используют для своих целей широкий спектр новых медиа-технологий[2].

В докладе Европола отмечается, что правые экстремисты активно перенимают тактику ведения пропаганды и вербовки у джихадистских группировок[3]. При этом, в отличие от последних, они пользуются гораздо большей свободой в основных социальных сетях.

Сайты и форумы праворадикальной направленности предоставляют поддержку и возможность общаться с единомышленниками, обеспечивают распространение указаний и инструкций по совершению террористических атак. В отсутствие физических ограничений, подобных международным границам, люди получают свободный доступ к экстремистским материалам, возможность легко

---

1 TE-SAT.

2 *Weimann G., Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace // International Institute for Counter-Terrorism. 05/04/2020. URL: https://www.ict.org.il/Article/2528/The_Virus_of_Hate#gsc.tab=0 (дата обращения: 20.05.2020); *Conway M.* Principal platforms and technologies of the global right-wing extremism ecosystem in Advisory network on terrorism and propaganda workshop: «Defining the global right-wing extremist movement» // EUROPOL. 17 Dec 2019. URL: https://www.europol.europa.eu/newsroom/news/advisory-network-terrorism-and-propaganda-workshop-“defining-global-right-wing-extremist-movement” (дата обращения: 07.10.2020).

3 TE-SAT.

обмениваться ими и заводить новые знакомства с единомышленниками. Все это существенно повышает риск их радикализации. Интернет привлекает правых экстремистов тем, что в сети легче сохранить анонимность и избежать контроля или вмешательства правоохранительных органов.

Онлайновые пространства укрепляют международные связи между правыми экстремистами. Правые экстремисты все активнее выстраивают отношения с единомышленниками за рубежом, в том числе на виртуальных платформах. Эти отношения позволяют правым экстремистам изучать новые методы работы и адаптироваться к новым условиям, например к новому национальному законодательству[1].

Английский язык является главным языком общения транснационального правого экстремистского сообщества. Например, террорист из немецкого города Галле использовал английский язык для обращения к воображаемой аудитории во время прямой трансляции атаки. Сайты шведских неонацистских организаций, в частности сайт «Nordfront» Скандинавского движения сопротивления и сайт «Нордической силы», также содержат англоязычные разделы.

Другие сайты ориентированы на определенные языковые группы. К их числу относится сайт франкоязычного движения белых сторонников превосходства «Suavelos», созданный в 2016 г. Как и многие другие праворадикальные сайты, сайт *Suavelos* претендует на роль новостного агрегатора. Однако выбирая тенденциозные новости, смешивая информацию из солидных и сомнительных источников и предоставляя ангажированные комментарии, он старается направить своих пользователей по пути радикализации и экстремизма. Кроме того, *Suavelos* обеспечивает безопасную площадку для белых супрематистов, чьи сообщения были удалены на основных платформах, таких как *Facebook* и *YouTube*, после атак в Крайстчерче. Со своего веб-сайта движение обращается к социальным сетям, например, создавая вторичные учетные записи на *Facebook* или каналы в *Telegram* с целью привлечения аудитории за пределами националистического сообщества[2].

Правый экстремистский онлайн-дискурс использует интернет-культуру троллей, с присущим ей использованием сарказма и ин-

---

1 TE-SAT.

2 *Sénécat A.* La galaxie Suavelos, vitrine d'un racism décomplexé // Le Monde. 11 Sept 2019. URL: https://www.lemonde.fr/les-decodeurs/article/2019/09/11/la-galaxie-suavelos-vitrine-d-un-racisme-decomplexe_5509154_4355770.html (дата обращения: 08.01.2021).

синуаций, как в целях манипулирования политическими оппонентами, так и для того, чтобы избежать личной ответственности за разжигание ненависти и подстрекательство к насилию. Ненавистнические высказывания, теории заговора и дегуманизация используются для приписывания негативных черт отдельным лицам или группам, таким образом делая их «законными» объектами насилия. Как часть культуры прославления террористов и нападающих, изображения и особые черты преступников включены в кодекс правил, используемый среди правых экстремистов[1].

По сообщениям СМИ, члены праворадикальных экстремистских сетей создают и используют мемы для распространения в качестве пропаганды с целью проникновения в массовую культуру с неонацистской повесткой дня[2]. Одна бельгийская ультраправая организация подозревается в том, что она создала «армию троллей» для поддержки своей пропаганды, публикуя скоординированные ненавистнические и угрожающие комментарии на странице онлайн-публикации или пользователей *Facebook*. Эти тролли также практикуют «доксинг», т.е. сбор открытой или полученной путем взлома информации о своих противниках с целью запугивания (под угрозой обнародования сведений). Кроме того, они продвигают свои собственные публикации, генерируя большие потоки обращений к ним через поддельные профили, ботов или используя услуги, предлагаемые «фермами кликов»[3].

Ключевые каналы праворадикальной пропаганды в сети. В настоящее время крайне правые активно используют веб-сайты, онлайн-дискуссионные форумы и псевдоновостные сайты для распространения своей идеологии[4]. Еще один компонент инструментария праворадикалов — набор относительно новых и очень доступных коммуникационных «приложений». Многие из них подпадают под категорию так называемых «темных социальных сетей» (*dark social*) — используемых экстремистами коммуникационных платформ, передаваемый через которые контент трудно отследить

---

1 *Kaati L., Asplund Cohen K., Akrami N., Shrestha A., Fernquist J., Pelzer B., Welander F., Isbister T.* 'Digitalt slagfält' // Swedish Defence Research Agency (FOI). 24 Oct 2019. URL: https://www.foi.se/report-summary?reportNo=FOI-R-4813-SE (дата обращения: 07.10.2020).

2 *Makuch B., Lamoureux M.* Neo-Nazis Are Organizing Secretive Paramilitary Training Across America // VICE News. 20 Nov 2018. URL: https://www.vice.com/en_us/article/a3mexp/neo-nazis-are-organizing-secretive-paramilitary-training-across-america (дата обращения: 07.10.2020).

3 TE SAT.

4 Там же.

путем средств мониторинга сети. К ним относятся, в частности, переписка в мессенджерах и закрытые групповые чаты. Обсуждаемые онлайн-ресурсы и приложения включают *Facebook*, *Twitter*, *YouTube*, *Gab*, *Reddit*, *4Chan*, *8Chan*, *Telegram*, *Discord* и *Twitch*[1]. Рассмотрим по порядку основные группы используемых платформ.

1. *Основные социальные сети*. Несмотря на усилия по выявлению и удалению контента сторонников белого превосходства, основные социальные медиа-платформы (*Facebook*, *Twitter*, *YouTube*) остаются важными источниками распространения правого экстремизма.

Facebook является крупнейшей социальной сетью в мире, в 2020 г. насчитывавшей более 2,6 млрд пользователей. Благодаря своей популярности *Facebook* стал важным инструментом для политических или общественных организаций и коммерческих брендов, включая, к сожалению, и ультраправых экстремистов. Несмотря на то, что компания явно запрещает разжигание ненависти и группы ненависти в своих правилах сообщества, *Facebook*, похоже, сталкивается с реальной проблемой, связанной с удалением контента неонацистов и сторонников белого превосходства со своей платформы[2].

Как отмечается в статье экспертов НКО «Avaaz» — организации, объединяющей международных интернет-активистов, была обнаружена сеть крайне правых учетных записей *Facebook*, распространяющая фейковые новости и ненавистнические высказывания среди миллионов людей по всей Европе. Поиск выявил более 500 крайне правых групп и страниц *Facebook*, работающих во Франции, Германии, Италии, Великобритании, Польше и Испании. Большинство из них использовали фальшивые страницы и профили для искусственной накрутки просмотров и распространения контента участников или сторонних сайтов, поддерживаемых ими, что нарушало правила *Facebook*. Публикации варьировались от французских аккаунтов, на которых размещался контент о превосход-

[1] *Weimann G.*, *Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace // International Institute for Counter-Terrorism. 05/04/2020. URL: https://www.ict.org.il/Article/2528/The_Virus_of_Hate#gsc.tab=0 (дата обращения: 20.05.2020); *Conway M.* Principal platforms and technologies of the global right-wing extremism ecosystem in Advisory network on terrorism and propaganda workshop: «Defining the global right-wing extremist movement» // EUROPOL. 17 Dec 2019. URL: https://www.europol.europa.eu/newsroom/news/advisory-network-terrorism-and-propaganda-workshop-“defining-global-right-wing-extremist-movement” (дата обращения: 07.10.2020).

[2] *Weimann G.*, *Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace.

стве белой расы, до публикаций в Германии, отрицающих холокост, и фальшивых страниц, рекламирующих вечеринку правой партии «Альтернатива для Германии» («AfD»).

Интересная тактика использовалась в Италии. Там праворадикалы создали сеть аккаунтов, посвященных широкому спектру тем — красота, здоровье, футбол и пр., которые затем постепенно трансформировались в политические инструменты трансляции своих взглядов[1].

Кроме того, правые экстремисты использовали возможности ведения прямых стримов через *Facebook live*. Этим воспользовался новозеландский террорист Брентон Таррант, ведя прямую трансляцию своего жестокого нападения. Мы еще вернемся к данному эпизоду.

Сеть микроблогов *Twitter* по-прежнему очень популярна в западном мире и остается важным каналом политического дискурса. Поэтому крайне правые стараются активно задействовать ее для трансляции своих нарративов. Выше приводилась статистика из исследования Института стратегического диалога, продемонстрировавшая трехкратное увеличение объема твитов, упоминающих теорию великого замещения, за период с 2014 по 2018 г. Кроме того, ученые установили почти 70 тыс. подписчиков аккаунтов «Поколения идентичности» в «Твиттере». Среди них лидируют учетные записи идентитаристов Германии, Австрии и Франции (соответственно 23,3 тыс., 16,5 тыс. и 13,2 тыс. подписчиков)[2].

YouTube остается самым известным и популярным видеохостингом в мире. Данная платформа позволяет пользователям просматривать и загружать видеоклипы, оценивать их, делиться, добавлять в плейлисты, отмечать, сообщать о видео, комментировать и подписываться на других пользователей. *YouTube* более популярен среди подростков, чем *Facebook* и *Twitter*.

Видеоплатформы, такие как *YouTube*, часто используются экстремистами для распространения своих взглядов, разжигания ненависти и даже для распространения трансляций нападений в прямом эфире. Некоторые молодые люди обнаруживают праворадикальный контент на *YouTube* случайно, в то время как другие ищут его. Автоматизированный рекомендательный алгоритм видеохостинга, ко-

---

[1] *Graham-Harrison E.* Far-right Facebook groups 'spreading hate to millions in Europe' // The Guardian. 22 May 2019. URL: https://www.theguardian.com/world/2019/may/22/far-right-facebook-groups-spreading-hate-to-millions-in-europe (дата обращения: 06.09.2020).

[2] *Davey J., Ebner J.* "The Great Replacement": the violent consequences of mainstreamed extremism.

торый после просмотра некоторых видеороликов предлагает схожие с ними, способствует вовлечению пользователей в экстремистскую воронку[1]. Пользователь может начать со случайного ролика о расизме и затем медленно, но верно продолжить погружаться в ультраправую «пучину». По мнению экспертов «Bellingcat», *YouTube* является наиболее частой причиной «красного пилинга» («*red-pilling*») участников. Этот жаргонный онлайн-термин означает обращение к крайне правым убеждениям[2]. Кроме того, механизм монетизации видео в *YouTube* позволяет крайне правым блогерам зарабатывать на распространении ультраправого контента.

Интересно, что в докладе Европола помимо основных западных сетей упоминается задействование правыми экстремистами в Европе и российской социальной сети «ВКонтакте». В частности, такой факт был зафиксирован в 2019 г. в Италии со стороны экстремистской организации «Римский арианский орден» (*Ordine Ario Romano*)[3]. От себя отметим, что присутствие западных ультраправых движений в сети «ВКонтакте» гораздо шире. В ходе написания статьи в поисковой выдаче неоднократно обнаруживались подобные тематические паблики на иностранных языках. Однако они были не слишком многочисленными и демонстрировали низкую вовлеченность подписчиков.

В последнее время администрации крупных социальных платформ стали активно зачищать правый экстремистский контент и его распространителей. Красной чертой стал теракт в Крайстчерче, прямой стрим и последующая видеозапись которого быстро распространялись через крупные социальные сети и достигли огромной аудитории. Так, *Facebook* после теракта объявил о борьбе с распространением идеологии «белого превосходства»[4]. *Twitter* за-

---

1 *Reed A., Whittaker J., Votta F., Looney S.* 'Radical Filter Bubbles: Social Media Personalisation Algorithms and Extremist Content' // The Global Research Network on Terrorism and Technology, Technology, Terrorism, 26 July 2019. URL: https://rusi.org/publication/other-publications/radical-filter-bubbles-social-mediapersonalisation-algorithms-and (дата обращения: 07.07.2020).

2 *Evans R.* From Memes to Infowars: How 75 Fascist Activists Were "Red-Pilled" // Bellingcat, 11 Oct 2018. URL: https://www.bellingcat.com/news/americas/2018/10/11/memes-infowars-75-fascist-activists-red-pilled/ (дата обращения: 06.09.2020).

3 TE-SAT.

4 *Conway M., Scrivens R., Macnair L.* 'Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends', ICCT Policy Brief // The International Centre for Counter-Terrorism. 25 Nov 2019. URL: https://icct.nl/publication/right-wing-extremists-persistent-online-presence-history-and-contemporary-trends (дата обращения: 06.09.2020).

явил, что «очистил» свою платформу в декабре 2017 г. Однако эффективность действий администрации социальных сетей вызывает у специалистов вопросы.

Например, *Facebook* для поиска и удаления праворадикального контента использует технологии экспертных оценок и технологии искусственного интеллекта, а также другие инструменты, такие как технологии сопоставления видео (*video-matching technology*) и поиска по ключевым словам (*language detection*). Однако проведенный внешними экспертами аудит механизма модерации контента выявил его недостаточную эффектность, когда значительная часть экстремистского контента оставалась на платформе после проведенной «зачистки»[1].

2. *Специализированные правые экстремистские новостные сайты и платформы.* В последние годы возникла альтернативная медиа-экосистема, которая явно обслуживает крайне правые сообщества. Не связанные редакционными принципами, как и традиционные печатные СМИ, эти источники используют комбинацию дезинформации, теорий заговора, чрезмерно пристрастных комментариев и подборку сенсационных историй для укрепления экстремистского мировоззрения.

Сторонники крайне правых убеждений создают собственные тематические сайты либо внедряются в уже существующие и перехватывают их содержательную повестку. Такие ресурсы служат безопасными сетевыми убежищами для правых экстремистских движений[2].

Например, широкую известность имеют такие сайты, как *Stormfront* и *Daily Stormer*. Ресурс *Stormfront* создан в 1995 г. американским белым супрематистом Доном Блэком (Don Black) и считается старейшим сайтом сторонников белого превосходства (причем до этого он уже несколько лет работал как электронная доска объявлений). Логотипом сайта является кельтский крест, внутри которого написана фраза «Белая гордость в мировом масштабе» (*White Pride World Wide*)[3]. На сайте размещались многочисленные материалы и велись активные дискуссии между пользователями по темам превосходства белой расы, нацизма и антисемитизма.

---

1 The Far Right on Facebook // Counter Extremism Project (CEP), 2019. URL: https://www.counterextremism.com/sites/default/themes/bricktheme/pdfs/The_Far_Right_on_Facebook.pdf (дата обращения: 06.09.2020).

2 TE-SAT; *Conway M.*, *Scrivens R.*, *Macnair L.* 'Right-Wing Extremists' Persistent Online Presence.

3 Stormfront // Anti-Defamation League. URL: https://www.adl.org/education/references/hate-symbols/stormfront (дата обращения: 17.01.2021).

Правозащитная организация «Южный правовой центр по вопросам бедности» (*Southern Poverty Law Center*) в 2000-е гг. называла *Stormfront* самый влиятельным ненавистническим сайтом в сети. Число его подписчиков в 2015 г. достигало 300 тыс. человек[1].

Однако в 2016 г. он утратил пальму первенства, которая перешла к экстремистскому ультрапраправому сайту нового поколения *Daily Stormer*. В его названии явно содержится отсылка к газете «Штурмовик» (*Der Stürmer*), издававшейся в нацистской Германии. Сайт был создан в 2013 г. американским неонацистом Эндрю Энглиным[2]. Сделав ставку на цепляющие заголовки и использование мемов, *Daily Stormer* сумел привлечь молодых сторонников неонацистских взглядов. Ресурс также известен кампаниями травли и троллинга, которые проводили его читатели в отношении своих идейных противников или недостаточно радикальных сторонников правых убеждений. Причем эти акции часто выходили за рамки виртуального пространства и перетекали в реальную жизнь.

Среди читателей *Stormfront* и *Daily Stormer* было немало известных неонацистов, впоследствии совершивших теракты, в том числе Андерс Брейвик, Дилан Руф и др.

Помимо откровенных неонацистских интернет-ресурсов, в сети существует множество иных альтернативных сайтов правой направленности, степень радикальности которых значительно ниже. В основном эти информационные ресурсы относятся к так называемым «альтернативно правым». В США таковыми являются популярные новостные консервативные и крайне правые ресурсы *Breitbart.com* и *Drudge Report*, сайты идеологического плана *AltRight.com* и *RADIX JOURNAL*, созданные видным активистом альтправых Ричардом Спенсером (Richard B. Spencer), сайт конспирологической направленности *InfoWars.com* известного радиоведущего и конспиролога Алекса Джонса (Alex Jones).

В Европе в основном преобладают новостные и концептуально-идеологические ресурсы крайне правого толка. Среди них можно отметить французские интернет-сайты *Riposte laïque* («Светский отпор») и *Résistance Républicaine* («Республиканское сопротивление»), продвигающие идеи в защиту светского государства и выступающие против исламизации Европы. В исследовании

---

[1] Hatewatch Staff. Don Black's Stormfront turns 20 // Southern Poverty Law Center. 27 Mar 2015. URL: https://www.splcenter.org/hatewatch/2015/03/27/don-blacks-stormfront-turns-20 (дата обращения: 17.01.2021).

[2] Eye of the Stormer // Southern Poverty Law Center. 9 Feb 2017. URL: https://www.splcenter.org/hatewatch/2015/03/27/don-blacks-stormfront-turns-20 (дата обращения: 17.01.2021).

Института стратегического диалога отмечается их ключевая роль в продвижении теории великого замещения[1].

Мощное информационное присутствие имеют представители Идентитаристского движения. Помимо многочисленных сайтов «Поколения идентичности», включая головной франкоязычный сайт *Generation Identitaire*, германоязычный сайт *Identitäre Bewegung* и др., для продвижения идей идентитаристы используют и тематические сайты, такие как франкоязычные новостные ресурсы *Novopress* и *Breizh-Info* и австрийский интернет-журнал *Info-Direkt*. Есть и более узкоцелевые ресурсы. Например, немецкое движение идентитаристов (*Identitäre Bewegung Deutschland*) запустило в 2020 г. сайт «*Карта опасностей*» (*Gefährder Map*), на котором публикуются фотографии и персональные данные «исламистов» и «проповедников ненависти», а также интерактивная карта с геотегами «исламистских угроз. На ресурсе имеется также специальная форма, с которой посетители сайта могут «сообщить об угрозе» посредством заполнения короткой анкеты.

Интересно, что немецкие идентитаристы даже запустили специальное приложение для мобильных и настольных устройств *Okzident News* — агрегатор новостей, которое позволяет пользователю получать push-уведомления с содержащихся в подборке «патриотических» и «альтернативных» веб-сайтов.

3. *Альтернативные социальные сети и имиджборды*. Помимо основных коммуникационных платформ, правые экстремисты используют также несколько периферийных платформ. Это либо тематические праворадикальные экстремистские площадки (Gab, Voat, 8Chan), либо платформы, захваченные правыми экстремистами (Reddit, 4Chan).

Англоязычная сеть *Gab* была создана в 2016 г. как альтернативная площадка, где нет диктата политкорректности и приветствуются любые выступления, независимо от того, насколько они вредны или оскорбительны. Поэтому Gab быстро стал безопасным пристанищем для крайне правых движений, которые продвигают экстремистский контент на данной платформе[2]. Платформа привлекла в себе внимание осенью 2018 г., когда устроивший стрельбу в синагоге Питтсбурга Р. Бауэрс опубликовал перед этим серию по-

[1] *Davey J., Ebner J.* "The Great Replacement": the violent consequences of mainstreamed extremism.

[2] TE-SAT.

стов в *Gab* с антисемитскими высказываниями и рассказал о своем намерении утроить теракт[1].

Популярный в западном мире социальный новостной сайт *Reddit* и его менее известный клон *Voat*[2] активно использовались крайне правыми для трансляции своих идей в силу мягкой цензурной политики. Например, *Voat* сохранял возможность публикации постов сторонниками конспирологической теории «QAnon» даже после того, как такой контент запретили на большинстве других платформ. Однако данный ресурс прекратил свою работу в конце 2020 г., сославшись на отсутствие средств[3].

В контексте нашего исследования следует упомянуть американскую социальную сеть *Parler*, которая получила широкую популярность в США среди сторонников президента страны Д. Трампа, консерваторов и крайне правых. Она позиционировалась как альтернатива *Twitter*. Однако после штурма Капитолия толпой праворадикалов компания «Big Tech» удалила приложение *Parler* из магазинов «AppStore» и «PlayMarket» и отключила его от хостинга.

Еще один тип платформ — *молодежные сетевые имиджборды*, включая *4Chan*, — активно задействовались праворадикальной средой в основном для публикации мемов и троллинга оппонентов. Но востребованный среди ультраправых имиждборд *8Chan* был использован в 2019 г. несколькими правыми экстремистами для размещения своих «манифестов», в которых они объясняли свои действия и призывали единомышленников совершать нападения. Это касалось нападений 15 марта в Крайстчерче (Новая Зеландия), 27 апреля в Пауэе (Калифорния, США) и 3 августа в Эль-Пасо (Техас, США). 10 августа исполнитель теракта в Беруме (Норвегия) опубликовал заявление о совершенном нападении на *Endchan*, еще одной производной платформе *Chan*. В то время как резервные производные версии платформы *Chan*, как сообщается, еще сохранялись в сети в конце 2019 г., хотя и не индексировались поисковыми системами, значительное число пользователей

---

1 *Roose K.* On Gab, an Extremist-Friendly Site, Pittsburgh Shooting Suspect Aired His Hatred in Full // The New York Times. 28 Oct 2018. URL: https://www.nytimes.com/2018/10/28/us/gab-robert-bowers-pittsburgh-synagogue-shootings.html (дата обращения: 19.01.2021).

2 Его нередко называли «Reddit альтернативных правых».

3 *Robertson A.* 'Free speech' Reddit clone Voat says it will shut down on Christmas // The Verge. 22 Dec 2020. URL: https://www.theverge.com/2020/12/22/22195115/voat-free-speech-right-wing-reddit-clone-shutdown-investor (дата обращения: 20.01.2021).

мигрировало на другие пиринговые зашифрованные платформы, такие как *Telegram* или *Discord*[1].

4. *Закрытые группы в мессенджерах и иные проявления «темных социальных сетей»* (*dark social*). Термин «Dark Social», который можно перевести как темные социальные сети, используется в маркетинге для описания материалов, распространение которых трудно отслеживать, таких как электронные письма, смс-сообщения и зашифрованные чаты. В контексте темы правого экстремизма он обычно применяется, чтобы обозначить каналы, используемые экстремистами для коммуникации, которые сложно анализировать с помощью традиционных инструментов анализа социальных медиа[2]. К ним относятся прежде всего мессенджеры и электронная почта.

Экстремистами преимущественно используются закрытые чаты и паблики в мессенджерах, доступ к которым осуществляется по личному приглашению, рекомендации других участников или после предоставления доказательств лояльности. Такие площадки чаще всего используются для обсуждения правых идей, координации и подготовки коллективных акций, а также планирования нападений. Как отмечается в докладе TE-SAT, закрытые коммуникационные пространства, например, предоставляемые мессенджером *WhatsApp*, сыграли важную роль в формировании правых террористических ячеек, ликвидированных в 2019 г. Кроме того, Швейцария сообщила, что она предотвратила одно нападение в мае 2019 г., когда несовершеннолетний был арестован по подозрению в планировании убийства мусульман и совершении нападений на мечети в стране. Подозреваемый общался с иностранными правыми экстремистами в *Instagram* (и, вероятно, в других социальных сетях)[3].

Однако в контексте правового экстремизма в США и Европе чаще упоминаются другие мессенджеры, а именно *Telegram* и *Discord*. Например, в докладе по теории великого замещения говорится о том, что «в зашифрованных мессенджерах *Discord* и *Telegram* радикальные группы, распространяющие идеологию белого геноцида, включают каналы “Поколения идентичности”, а также международные альт-правые группы»[4].

---

1 TE-SAT.

2 *Davey J., Ebner J.* “The Great Replacement”: the violent consequences of mainstreamed extremism.

3 TE-SAT.

4 *Davey J., Ebner J.* “The Great Replacement”: the violent consequences of mainstreamed extremism.

Мессенджер *Telegram* был создан Павлом Дуровым, основателем социальной сети «ВКонтакте». Шифрование переписки, опция секретных чатов, удобные групповые чаты и каналы, а также ставка на анонимность и активное препятствование администрации мессенджера получению данных со стороны спецслужб привлекли к нему внимание и экстремистов, в том числе крайне правых.

Мощный приток сторонников консервативных взглядов в *Telegram* состоялся после блокировки аккаунта Трампа в основных социальных сетях и прекращения работы ресурса *Parler* в январе 2021 г. Интересно, что американские неонацисты и белые супрематисты посчитали данный момент знаковым и направили большие усилия на вербовку в свои ряды сторонников Дональда Трампа[1].

Что касается *Discord*, то он был изначально запущен как мессенджер для геймеров с поддержкой голосовой и видеосвязи. Однако групповые чаты и каналы быстро освоили белые супрематисты и прочие крайне правые. *Discord* привлек их своими параметрами конфиденциальности и анонимности, позволяющими пользователям создавать закрытые группы чатов со входом по приглашениям, невидимые для окружающих[2]. Однако после беспорядков в Шарлотсвилле, организованных ультраправыми активистами в августе 2017 г., в ходе которых один из них совершил целенаправленный наезд на участников группы противников марша, администрация платформы предприняла активные меры по удалению каналов и чатов ультраправых. Поводом к этому стали активное обсуждение и координация действий участников данного марша в мессенджере. «Жалкие ботаники из Discord сдались и присоединились к войне против свободы слова. Но мы сумеем приспособиться», — так отреагировали на решение руководства платформы *Discord* сторонники крайне правых убеждений в посте на сайте

[1] *Criezis M.* Redpill the “Parler Refugees”: White Supremacist Strategies for Radicalising Trump Supporters on Telegram // Global Network on Extremism & Technology. 18 Jan 2021. URL: https://gnet-research.org/2021/01/18/redpill-the-parler-refugees-white-supremacist-strategies-for-radicalising-trump-supporters-on-telegram/?fbclid=IwAR1Xv0N2M4t8ydegQwZODTW4oCqRLDDgWPjVlgaAR8qdBEUki28P-bEC3sc (дата обращения: 20.01.2021)

[2] *Roose K.* This Was the Alt-Right’s Favorite Chat App. Then Came Charlottesville // The New York Times. 15 Aug 2017. URL: https://www.nytimes.com/2017/08/15/technology/discord-chat-app-alt-right.html (дата обращения: 19.01.2021).

AltRight.com[1]. В итоге произошла частичная миграция ультраправых на другие площадки, включая *Telegram*, *Signal* и др., однако они все равно продолжают использовать *Discord*.

Необходимо сделать одну оговорку. Мессенджеры *Telegram* и *Discord* популярны в праворадикальной среде не только из-за своих приватных индивидуальных и групповых чатов, но и из-за публичных каналов и групп. И с таким функционалом их стоит рассматривать в качестве альтернативных социальных медиа крайне правых (группа 3, обозначенная выше).

Отдельно следует упомянуть приложение *Patriot Peer* («Радар патриота»), самостоятельно разработанное Идентитаристским движением и представленное Мартином Зельнером. *Patriot Peer* представляет собой социальный сервис, сочетающий возможности *Tinder* и *Pokemon Go* и позволяющий членам движения обнаруживать друг друга поблизости на карте и встречаться для общения. Сервис имеет элементы геймификации, присваивая и накапливая баллы для наиболее активных его участников[2].

Пропаганда действием: террористические атаки и их медийное освещение

Мощнейшим пропагандистским эффектом для глобального праворадикального сообщества обладают активные экстремистские действия, прежде всего теракты. Резонансные нападения правых экстремистов вдохновляют других сторонников и снижают тем самым порог проявления насилия. Аналогичный тренд наблюдался и в джихадистском терроризме.

Наиболее известным и прославляемым терактом в праворадикальном сообществе долгое время считались атаки Андерса Брейвика в Норвегии в 2011 г., когда в результате подрыва бомбы в столице и последующего массового расстрела острова Утёйа погибло 77 человек и свыше 150 получили ранения. Брейвик стал по-настоящему культовой фигурой крайне правых экстремистов.

Именно теракты Брейвика вдохновили Брента Тарранта на совершение своего жестокого нападения в Крайстчерче, жертвами

[1] *Roose K.* This Was the Alt-Right's Favorite Chat App. Then Came Charlottesville // The New York Times. 15 Aug 2017. URL: https://www.nytimes.com/2017/08/15/technology/discord-chat-app-alt-right.html (дата обращения: 19.01.2021).

[2] *Prinz M.* „PATRIOT PEER" ALS MISCHUNG AUS TINDER UND POKEMON GO // Bell Tower news. 28 Feb 2017. URL: https://www.belltower.news/heimatliebe-im-app-store-patriot-peer-als-mischung-aus-tinder-und-pokemon-go-43312/ (25.01.2021).

которого стали 51 человек погибших и 49 раненых. Данный теракт стал еще более «вирусным» и повлек за собой в короткий период большое число действий подражателей. Только в 2019 г. в мире под влиянием действий новозеландского стрелка было совершено пять терактов. Их география охватывает США и страны Западной и Северной Европы (Великобритания, Германия, Норвегия).

Одна из причин наблюдающейся тенденции роста волны нападений правых экстремистов, вдохновленных терактами Брейвика, Тарранта и других праворадикалов, состоит в особом характере подготовки и совершения данных преступлений, рассчитанных на создание широкого общественного и медийного резонанса. Здесь можно выделить несколько составляющих.

Во-первых, был выбран достаточно «зрелищный» способ совершения терактов — массовый расстрел. Преступники, вооружившись автоматическим оружием и большим количеством боеприпасов, продолжительное время хладнокровно передвигались и методично расстреливали попадавшихся им по пути беззащитных людей. В этом способе есть что-то и от голливудских боевиков, и от компьютерных шутеров. К тому же на винтовки Тарранта белыми буквами были нанесены упоминания об исторических событиях, личности и лозунги, связанные с противостоянием мусульман и христиан.

Во-вторых, и Брейвик, и Таррант остались живы и были задержаны полицией. Последовавший затем длительный судебный процесс обеспечил долгое медийное освещение совершенных ими преступлений и личностей самих террористов в течение продолжительного времени. Медиа транслировали кадры из зала суда, сделанные подсудимыми заявления в ходе процесса, привлекая к ним дополнительное общественное внимание.

В-третьих, оба названных террориста опубликовали перед началом своих нападений в сети пространные манифесты, в которых изложили свою идеологию и объяснили причины, побудившие их к насилию. Брейвик накануне теракта разослал пространный 1514-страничный манифест под названием «2083-Декларация независимости Европы» (2083-A European Declaration of Independence) и разместил на *YouTube* 12-минутный презентационный видеоролик с аналогичным названием. Таррант подготовил свой манифест под названием «Великое замещение», который незадолго до начала стрельбы отправил получателям по электронной почте и разместил ссылки на него в социальной сети *Twitter* и имиджборде *8chan*. В манифесте он утверждал, что его нападения стали местью за совершенные террористические акты в Европе и пред-

полагаемый геноцид белых европейцев. Публикация манифестов стала отличительной чертой атак правых экстремистов последнего времени.

Есть еще один очень важный момент, который характерен только для теракта в Новой Зеландии. Брентон Таррант заранее анонсировал и вел прямую трансляцию своего теракта на *Facebook* с помощью экшн-камеры. На видео нападавший комментировал ход атаки, как бы выступая перед аудиторией, и демонстрировал свое оружие, на котором были начертаны имена исторических личностей и сражения в борьбе европейских держав против Османской империи. Атака транслировалась в прямом эфире в течение 17 минут и просматривалась не менее 4000 раз, прежде чем *Facebook* отключил ссылку. В течение следующих 24 часов *Facebook* удалил еще 1,5 млн копий видео атаки со своих страниц.

Насколько нам известно, это был первый в истории теракт с прямой онлайн-трансляцией (хотя отдельные прецеденты отрывочных прямых стримов с мест событий были зафиксированы и ранее). Видеозаписи с камеры новозеландского стрелка потом массово распространялись в социальных сетях, хотя администрация платформ старалась оперативно их удалять. Исследователи усмотрели в данном инциденте элемент геймификации терроризма (внедрения игровых сюжетов и техник), что проявилось в схожести прямой трансляции теракта в Крайстчерче с онлайн-стримами прохождения компьютерных игр, популярных в молодежной среде[1].

Данное техническое новшество несомненно будет востребовано и в последующем. Показательно, что вдохновленный новозеландским терактом мужчина, совершивший нападение на синагогу в американском Пауэе 27 апреля 2019 г., также планировал вести его онлайн-трансляцию в Facebook[2], а исполнитель теракта в не-

[1] *Schlegel L.* Points, Rankings & Raiding the Sorcerer's Dungeon: Top-down and Bottom-up Gamification of Radicalisation and Extremist Violence // Global Network on Extremism & Technology. 17th February 2020. URL: https://gnet-research.org/2020/02/17/points-rankings-raiding-the-sorcerers-dungeon-top-down-and-bottom-up-gamification-of-radicalization-and-extremist-violence/ (дата обращения: 21.09.2020).

[2] *McGowan M.* San Diego shooting suspect posted 'open letter' online // The Guardian, 28 April 2019. URL: https://www.theguardian.com/us-news/2019/apr/28/john-earnest-san-diego-shooting-suspect-postedopen-letter-online (дата обращения: 17.01.2021).

мецком Галле такую трансляцию вел через игровую онлайн-платформу *Twitch*[1].

Таким образом, совершение резонансных терактов, спланированных в расчете на широкий медийный эффект и сопровождающихся распространением экстремистских манифестов, а в последнее время — и прямыми онлайн-трансляциями, является эффективным способом донесения своих посланий правыми экстремистами до глобальной аудитории. Подобная пропаганда действием способна порождать новые серии атак правых одиночек по всему миру. К тому же она усиливает прославление правых террористов, которые таким способом увековечивают свое имя в правом экстремистском сообществе (по аналогии с «солдатами халифата» ИГИЛ).

Влияние пандемии на информационную активность ультраправых

Пандемия коронавируса COVID-19, ставшая главным мировым событием 2020 г., заметно отразилась на сетевой пропаганде правых экстремистов. Она открыла для праворадикалов уникальные возможности сеять ненависть, страх, панику и хаос. По мере распространения вируса он становился доминирующим контентом в крайне правых СМИ и онлайн-чатах[2]. На крайне правых онлайн-платформах, таких как *Telegram* и *Gab*, и на более традиционных платформах, таких как *Instagram*, *Facebook* и *Twitter*, крайне правые группы и отдельные лица продвигали теории заговора, обвиняющие во всех бедах беженцев и обосновывавшие необходимость закрытия границ. Со времени вспышки в начале декабря 2019 г. на таких сайтах, как *Telegram*, *4chan* и *Gab,* коронавирус связывают с расистскими и антисемитскими оскорблениями и мемами. Контент варьировался от расистских постов до пародий на китайцев, осмеивающих их гигиену и привычки питания[3].

Среди крайне правых активно циркулировали конспирологические теории вокруг вируса. Как отмечает Р. Катц, эти теории часто возбуждали антисемитизм или ксенофобию против людей

---

1 *Koehler D.* 'The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat // CTC Sentinel. Dec 2019. Vol. 12. Is. 11. P. 14–20.

2 *Katz R.* The Far-Right's Online Discourse on COVID-19 Pandemic // SITE Intelligence Group. March, 2020 URL: https://ent.siteintelgroup.com/index.php?option=com_acymailing&ctrl=archive&task=view&mailid=20576&key=4lfGcEyn&subid=1472-t9ir9gm3ghmVr7&tmpl=component (дата обращения: 27.06.2020).

3 *Weimann G., Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace.

из Китая, поскольку обсуждали роль китайского правительства или «еврейской глобальной элиты» в этой вспышке. Использовался широкий спектр теорий заговора, в том числе обвиняющих евреев в создании и распространении вируса, в разработке вакцины, которую людям нужно отказаться принимать, а также в извлечении прибыли от пандемии. Другие заговорщики выдвигали теорию о том, что эта болезнь была произведена США и (или) Израилем в качестве биологического оружия для борьбы с такими соперниками, как Китай и Иран. Подобные обвинения звучат не впервые. Во время вспышки средневековой эпидемии чумы евреев также сделали «козлами отпущения», обвинив в умышленном отравлении колодцев[1].

Самым тревожным аспектом пропагандистской кампании, связанной с коронавирусом, стали прямые призывы к использованию инфекции в качестве биологического оружия. Зараженные люди должны «посетить вашу местную синагогу и обнять как можно больше евреев», говорилось в одном посте. Один крайне правый плакат также советовал «кашлять на представителей ваших местных меньшинств». Другой призывал к той же тактике против критически важной инфраструктуры: «кашляйте в местном транспорте»[2]. Федеральная служба защиты (*Federal Protective Service*), входящая в состав Министерства внутренней безопасности США, сообщила, что «белые расово мотивированные воинствующие экстремисты недавно прокомментировали коронавирус, заявив о наличии у своих сторонников обязательств распространять коронавирус в случае собственного заражения». В группе Telegram они обсуждали, как оставить “слюну на дверных ручках” и распространить ее среди своих “врагов”»[3].

Некоторые свои призывы ультраправые оформляли в виде графических материалов, таких как мультфильмы, плакаты и картинки. Один из таких постеров, которому фиктивно приписали авторство Центра по контролю и профилактике заболеваний (CDC), побуждал людей посещать мечети или синагоги и ездить на общественном транспорте. Это противоречило реальным рекомендациям органов общественного здравоохранения и безопасности.

Поддельные новости, слухи, мистификации и теории заговора, которые были распространены во время пандемии коронавируса, не только отражают предрассудки в отношении азиатов, евреев,

1 *Katz R.* The Far-Right’s Online Discourse on COVID-19 Pandemic.
2 *Weimann G., Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace.
3 Ibid.

китайцев, иностранцев, иммигрантов, но и представляют их в причинно-следственном комплексе. Их прямо называют причинами появления вируса, поэтому их нужно обличать и наказывать. Политизация коронавируса крайне правыми указывает на то, как эти способы дискурса служат нарративами, которые усиливают расистские и антисемитские концепции и убеждения[1].

Кроме того, ситуация дезорганизации экономики и систем здравоохранения, а также повышенная тревожность общества были использованы ультраправыми для продвижения своих апокалиптических нарративов в духе теории акселерационизма (*accelerationism*). Эта теория основывается на идее, что восстановление расово чистого мирового порядка требует усиления социального хаоса, после чего начнется расовая война и станут возможными революционные изменения[2]. Поэтому правые экстремисты наводнили социальные сети и альтернативные платформы своими устрашающими рассказами о неизбежности крушения социума и начала расовой войны. «Этот ядовитый идеологический вирус крайне правых, — подчеркивают эксперты, — использует вызванную пандемией тяжелую ситуацию для подстрекательства к насилию в отношении определенных социальных групп, включая иммигрантов, меньшинства или либералов, которых делают козлами отпущения»[3].

* * *

Проведенный нами анализ показал, что правый экстремизм в странах Западного мира активно эволюционирует и набирает силу. Находясь определенное время в тени джихадистского терроризма ИГИЛ и подобных террористических группировок, оттянувших на себя внимание спецслужб, он расцвел в странах Запада. Важным фактором мобилизации ультраправых стало формирование разветвленной цифровой экосистемы, включающей аккаунты и сообщества в социальных сетях, тематические интернет-сайты и порталы, а также приватные каналы и чаты в мессенджерах.

Для роста праворадикальных настроений имелись и объективные причины — политические (усиление правоконсервативных настроений в обществе и приход к власти выражающих их политиков в США и ряде европейских стран, антиистеблишментная

[1] *Weimann G., Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace.

[2] *Wallner C., White J.* The Far-Right and Coronavirus: Extreme Voices Amplified by the Global Crisis // The Royal United Services Institute, RUSI. 30 Apr 2020. URl: https://rusi.org/commentary/far-right-and-coronavirus-extreme-voices-amplified-global-crisis (дата обращения: 14.06.2020).

[3] *Weimann G., Masri N.* The Virus of Hate: Far-Right Terrorism in Cyberspace.

волна), экономические (падение уровня жизни, деградация некоторых отраслей экономики, экономический урон от пандемии), социальные и культурные (активные миграционные процессы и вызванное ими увеличение доли населения с иными ценностными и поведенческими установками, усиление роли ислама в мире в целом и странах Запада, рост социальной поляризации и конфронтации различных социальных групп).

Новое поколение крайне правых движений на Западе, обозначаемое как альтернативно правые в США и новые правые в Европе, имеет гораздо меньшую степень радикализма и склонность к насилию, нежели наци-скинхеды и подобные им неонацисты, что позволяет им счистить прежний налет маргинальности и расширять свое политическое влияние в обществе. Этому способствуют также мощные идеологические нарративы, апеллирующие к экзистенциальной угрозе для западной цивилизации со стороны мигрантов из арабских и африканских стран, преимущественно исламского вероисповедания. Собранные в стройную концепцию великого замещения, данные идеи находят широкий общественный отклик.

Вместе с тем целенаправленные усилия западных политиков, СМИ и компаний технологической сферы (*Big Tech*) по навешиванию ярлыков неонацистов на любые правые движения и их дискредитации неизбежно толкают их в маргинальную нишу, где действительно существует множество профашистских и неонацистских структур. Таким образом относительно умеренное крыло крайне правых маргинализируют, содействуя тем самым его радикализации.

Несмотря на публичное отрицание насилия как инструмента решения проблем со стороны ведущих лидеров движений крайне правых на Западе, их глобальная виртуальная экосистема его неизбывно продуцирует. Однако теракт в Крайстчерче стал красной чертой, зайдя за которую, ультраправые вызвали жесткую реакцию правоохранительной системы западных стран. Мощный удар по их сетевой инфраструктуре был нанесен со стороны администрации социальных сетей, что заставило их искать новые безопасные убежища. В США альт-правые, среди которых немало откровенных неонацистов, навлекли на себя гнев властей и определенной части общества после массовых беспорядков и теракта в Шарлотсвилле, а также штурма Капитолия 6 января 2021 г.

Несмотря на общность проявлений и трендов развития правого экстремизма в США и Европе, полагаем, что в среднесрочной перспективе он будет развиваться по-разному в силу существенных различий в их ключевых детерминантах. Если в Европе таковыми

продолжат оставаться социальные конфликты, вызванные изменением этнического состава населения и возрастающей исламизацией общества, то в США корень проблем заключается в растущей пропасти и усиливающемся взаимном ожесточении между ультраправыми и ультралевыми движениями, имеющими выраженную расовую принадлежность и атрибуцию среди политических элит (это явно обозначилось в ходе президентской избирательной кампании 2020 г.). Учитывая наличие у американского населения большого количества огнестрельного оружия, властям придется предпринять серьезные усилия для того, чтобы предотвратить воплощение мрачного сценария гражданской войны в реальность[1].

[1] Disarray 2020: Inside the Far Right's Apocalyptic Prepping for Post-Election "Civil War" // SITE Intelligence Group. Oct 22, 2020. URL: https://ent.siteintelgroup.com/Special-Reports/disarray-2020-inside-the-far-right-s-apocalyptic-prepping-for-post-election-civil-war.html (дата обращения: 26.01.2021).

В.С. Овчинский

Терроризм и технологии XXI века: что должно быть под контролем оперативных подразделений? Европейский взгляд

Многие исследователи чрезмерно концентрируются на будущих возможностях использования современных технологий в деятельности террористических организаций, а не на их текущем применении. К сожалению, это уже не будущее, а повседневная реальность нашего времени. Об этом убедительно повествует ***доклад Института ЕС Новая Европа «Технологии и терроризм» (2021 г.)***.

Беспилотные летательные аппараты (БПЛА)

Террористические организации уже много лет пытаются использовать дроны. 2 октября 2016 г. они осуществили первую смертельную атаку с использованием БПЛА. ***ИГИЛ*** использовало вооруженный беспилотник, убив двух курдских боевиков и ранив французских солдат (*На наш взгляд, самые примитивные дроны использовались террористами гораздо раньше, примерно с 2013–2014 гг. — В.О.*).

В 2017 г. ИГИЛ уже объявило о создании специального подразделения под названием «Беспилотные летательные аппараты моджахедов», основной целью которого были разработка и использование БПЛА в рамках долгосрочной стратегии по развитию и вооружению беспилотных технологий. Группа использовала беспилотные летательные аппараты для наблюдения и наведения на цель, в основном в Ираке и Сирии. Несмотря на растущие потери территории, ИГИЛ постоянно совершенствуется в модернизации, производстве и развертывании БПЛА. В том же 2017 г. организации удалось нанести беспилотный удар по боевому танку в Мосуле.

В начале 2019 г. произошло беспрецедентное нападение: рой дронов атаковал два российских военных объекта в Сирии. Рассматриваемые беспилотники имели барометрические датчики, которые позволяли им изменять высоту, и высокоразвитую систему GPS-наведения с конкретными целями, которые были запрограммированы на уничтожение. Другими словами, дроны, которые участвовали в атаке, не требовали дальнейших инструкций или указаний со стороны террористов после их запуска. Десять таких бес-

пилотников были оснащены взрывными устройствами и упали над авиабазой Хмеймим, а три других были нацелены на российский военно-морской корабль боевой поддержки недалеко от Тартуса. Другое вооружение включало снаряды, начиненные тетранитратом пентаэритрита (ТЭН), которые прикреплялись к их крыльям. Что еще хуже, БПЛА летели на малых высотах и не могли быть обнаружены. Тем не менее их атаки были синхронизированы таким образом, что это сбивало с толку системы ПВО. В конце концов, атака, которая, вероятно, была подготовлена ***сирийской повстанческой группировкой***, провалилась. Российские системы отреагировали комплексным использованием кинетических и электронных систем защиты воздушного пространства.

Позже в том же году корабль, управляемый дистанционно ***хуситами***, атаковал нефтяные объекты Саудовской Аравии в Абкайке и Хурайсе. Повстанцы нацелились на крупнейший в мире нефтеперерабатывающий завод. Злоумышленники отправили от 10 до 25 дронов, которые выполнили операцию как рой. БПЛА атаковали по крайней мере двумя волнами и нанесли достаточно повреждений, поэтому тушение пожаров представляло собой серьезную проблему. Проверка спутниковых изображений показала, что было нанесено как минимум 19 ударов, в результате которых повреждено 14 контейнеров для хранения. Хотя Саудовская Аравия имеет системы противоракетной обороны MIM-104 Patriot, она не смогла обнаружить их из-за слишком низкого и под разными углами полета, что снова сделало ПВО неэффективной.

За 2019–2020 гг. были совершены сотни атак с использованием беспилотников и ракет на инфраструктуру Саудовской Аравии.

Такие типы атак — первый шаг, символизирующий, что технологические достижения могут позволить оружию (частично или полностью) самостоятельно разрушать инфраструктуру врага. Большинство стран, прогрессирующих в гонке искусственного интеллекта (ИИ), предлагают меньшие, более быстрые и практически автономные дроны, что со временем только увеличит серьезность будущих атак. В то же время правительства и частные компании контролируют эти виды передовых технологий, и из-за этого данные подвергаются значительному риску стать мишенью для шпионажа.

Террористы также используют БПЛА для получения информации о местонахождении вооруженных сил, типе вооружения или потенциальных передвижениях солдат. В этом отношении террористы действуют аналогично государственным силам. Владение передовыми технологиями позволяет им сражаться на более равных

основаниях с государственными силами (как и частные военные компании действуют аналогично государственным силам из-за владения передовыми технологиями).

Есть по крайней мере несколько факторов, которые приводят к частому использованию БПЛА преступными группами, террористами, сепаратистами или повстанцами.

Использование БПЛА на больших расстояниях. Большинство террористических групп могут проводить атаки с больших расстояний. Технология, позволяющая отслеживать цель, а также координировать действия с поставленной целью, — идеальное оружие для войны. Крупнейшие террористические организации имеют свои штаб-квартиры на Ближнем Востоке и в Африке или пытаются захватить часть территории в своем регионе. Если это регион, где они регулярно сталкиваются с армией государства, или он находится недалеко от границы, гораздо более рентабельно отправлять дроны с бомбами. Путь от штаб-квартиры террористической группы может быть непростым, но если есть возможность отправить БПЛА, это становится более легкой задачей. Наряду с этим превосходство в воздухе — ключевая тактика, которую используют многие государства в борьбе с террористами. Если организации достигают превосходства в воздухе за счет использования БПЛА, то это становится не только проблемой расстояния или логистики, но и проблемой умножения сил. В атаке с дальней дистанции с помощью дронов основная цель террористов — удивить противника, а затем нанести как можно больший урон, в идеале без использования собственных сил. ИИ, управляя дронами, может выследить, уничтожить цель и немедленно вернуться в укрытие террористов. В этом сценарии дальний бой с террористами никогда не был более правдоподобным.

Кроме того, террористы используют БПЛА как средство отвлечения внимания, чтобы провести аналогичную атаку в другом месте. Террорист может работать, чтобы захватить и подготовить несколько дронов для синхронной атаки в нескольких частях густонаселенных районов. В случае удара одного беспилотника власти отреагируют, и это будет повторяющаяся схема с последующим нанесением большего количества ударов беспилотником.

От злоумышленника может потребоваться физическое участие в атаке, а может и не потребоваться, поскольку ИИ сможет координировать и проводить атаку практически без участия террориста. Это также обеспечит террористу повышенную анонимность из-за того, что от него не требуется раскрывать себя, или более широкое окно возможностей для перемещения вдали от властей, бóльшую

выживаемость и, следовательно, шансы совершить больше атак в будущем.

Доступная цена на передовые технологии. Из-за технологической гонки и соперничества между могущественными странами гораздо более вероятно, что террористические группы получат дроны с ИИ. Развертывание этой технологии в США, Китае, России, Индии, Великобритании или Германии на местах приведет к более легкому доступу к этому оружию. В целом, сложность приобретения дронов с ИИ будет меньше, чем можно было бы предположить.

Глобальное участие сверхдержав в войнах на Ближнем Востоке и в Африке, а также постоянное совершенствование систем обороны и определение государственных интересов, сосредоточенных на экономической и региональной безопасности (с выделением, таким образом, дополнительных ресурсов в регионе), дает террористическим организациям возможность для приобретения такого оборудования, где это возможно. Это не случай «если», а вопрос «когда и против кого» они будут их использовать, что приводит к использованию террористами дронов с ИИ. Они приносят новую динамику на поле битвы с оружием, которое уже обычно используется государственными армиями. Благодаря своей находчивости террористы могут либо приобрести их самостоятельно, либо стать получателями этих технологий через государственную спонсорскую поддержку.

Стоимость покупки в будущем снизится до «приемлемого уровня», по крайней мере для нескольких террористических организаций, уже имеющих значительные финансовые средства для поддержки своих операций.

Нетребовательный процесс эксплуатации. Похоже, что террористы, скорее всего, не станут разрабатывать собственные ИИ и БПЛА, которые будут поставляться на международный рынок. Для такого длительного и «требовательного» с финансовой точки зрения процесса нет времени — террористы должны быть снабжены конкретным оружием, готовым к немедленному применению. Процесс приобретения зависит от поставщика, особенно когда у организации нет своей собственной отрасли или соответствующих инженеров.

Поскольку в будущем БПЛА будут оснащены ИИ, инженеры, знакомые с этим типом программного обеспечения, не столкнутся с трудностями в его модификации или адаптации, что позволит террористам с легкостью их использовать.

Маркировка террористической деятельности. Информация о террористах, причастных к атаке, осуществленной с помощью дронов с ИИ, может быть обнародована в зависимости от потребностей террористов, международного контекста и, прежде всего, от наличия достаточных доказательств для того, чтобы обвинить организацию, а не государственного провайдера.

Некоторые террористические организации, такие как «Исламское государство», «Аль-Каида», могут предпочесть оказать влияние и громко продемонстрировать свой новый успех. Это может быть сделано для того, чтобы объявить международному сообществу, что у них есть такое оружие и что они могут постоянно конкурировать с государственными армиями. Более того, они могли бы использовать свои первые атаки как средство распространения паники, угрожая своим врагам последующими набегами. Учитывая тенденцию террористических организаций демонстрировать присутствие и силу, они могут пометить свои дроны флагами или опубликовать информацию об их использовании в социальных сетях.

Улучшение противовоздушной войны. В последнее время развертывание дронов ускорилось на многих полях сражений. Проводятся новые испытания, которые повысят боевой потенциал боевых БПЛА во многих ситуациях, например при уничтожении или вводе в заблуждение средств ПВО. Преимущество использования неотслеживаемых БПЛА, управляемых ИИ, стало бы наиболее важным элементом собственного вооружения. Совершенно очевидно, что большинство стран, вовлеченных в конфликты, такие как конфликты в Сирии и Ливии, испытывают новое оружие. Более того, некоторые из этих попыток дали заметные результаты.

Неспособность устранить воздушную угрозу указывает на необходимость повышения эффективности их противовоздушной обороны. Это тесно связано с продолжающимися конфликтами, в которых используются новые технологии, что приводит к глобальной конкуренции в борьбе с зенитными системами.

Террористические организации, безусловно, будут пытаться заполучить эти виды современного оружия. Они стараются действовать на одном уровне с государственными «организмами», часто отмечая свое преступное присутствие. В качестве одного из многих примеров можно привести уже упомянутый: когда несколько нефтяных объектов Саудовской Аравии в сентябре 2019 г. подверглись ракетным ударам и ударам беспилотников, нанесенным повстанцами-хуситами.

Даже полностью оснащенные страны с мощным потенциалом безопасности могут стать жертвами террористических атак, что

приведет к потере человеческих жизней и целостности критически важной инфраструктуры, поскольку они могут подвергнуться возможному нападению. В настоящее время цели, особенно критическая инфраструктура, не могут функционировать, если противовоздушная оборона не сможет защитить их, а атакующие имеют в своем распоряжении широкий спектр вариантов электронного и кинетического оружия.

О войне дронов ближайшего будущего. Стаи дронов представляют огромную угрозу для оборонных систем государств во всем мире. Большое количество летательных аппаратов, готовых уничтожить противника, каждый из которых несет более 200 кг взрывчатых веществ, может оказаться сложной задачей. Некоторые дроны могут вести огонь из оружия, а другие могут одновременно сбрасывать бомбы, идеально выполняя миссию. Однако осуществить такую атаку с помощью людей, управляющих дронами, практически невозможно. Ни одно подразделение солдат не могло бы контролировать траекторию полета каждой машины в рое так эффективно, как ИИ. Только ИИ, который запускает атаку сам по себе, может управлять огромным количеством машин, избегая систем ПВО, идеально синхронизированным образом, сохраняя при этом контроль над своими активами. Кроме того, не исключено, что дроны скоро будут иметь боевую нагрузку до 10 тонн. Рой дронов, несущих по крайней мере несколько тонн взрывчатки, станет самым смертоносным оружием в мире, не считая ядерного оружия.

Помимо использования дронов с ИИ для увеличения своей мощности, террористы также могут оценить возможность использования их в целях анонимности. Например, чтобы человеческий фактор оставался скрытым при проведении атаки, закончившейся успехом или неудачей.

Вполне возможно, что по масштабам война дронов между государственными и негосударственными субъектами будет сродни битвам между военно-воздушными силами государств за утверждение господства в небе.

3D-печать

Как известно, 3D-печать — это процесс, с помощью которого можно создавать трехмерные твердые объекты любой формы и геометрии из цифрового файла. Есть несколько программ, которые позволяют составить проект с помощью программного обеспечения для 3D-моделирования. Объект может быть реплицирован на основе копирования существующей модели или построен с нуля. Как

правило, 3D-сканер, который находится внутри 3D-принтера, создает точную копию отсканированного физического объекта и загружает его схемы в виде цифрового файла.

Нынешнее развитие этой технологии, а также возможности использования ИИ приводят к популяризации многих высокотехнологичных систем, которые могут быть опасны в руках террористов.

Благодаря 3D-печати необходимое вооружение становится легко доступным для террористов. Однако оружие, напечатанное на 3D-принтере, не может быть заряжено пулей, которая не была адаптирована к оружию, — для этого требуется проверка прочности материалов. Кроме того, в большинстве случаев печатное оружие можно использовать только один раз, чтобы выстрелить короткой очередью ракет или одиночной пулей. Тем не менее тот факт, что террористы могут печатать оружие для себя в любой точке мира, представляет собой серьезнейшую угрозу безопасности. Качество 3D-печати повышается, а доступ к технологии увеличивает риск и эффективность террористов, использующих печатное оружие. Это может привести к увеличению числа террористических атак во многих странах из-за доступности данной технологии.

Одним из наиболее ярких примеров использования 3D-печати в террористических целях было ***нападение на синагогу в Галле****. Экстремист, которого опознали как 28-летнего гражданина Германии по имени Штефан Баллиет, решил совершить теракт во время еврейского праздника Йом Кипур 9 октября 2019 г. Он начал атаку, пытаясь проникнуть в синагогу, стреляя и используя самодельную взрывчатку. Когда экстремист не смог выбить дверь, он начал стрелять в прохожих рядом с храмом и убил одну женщину. Мужчина, который проходил мимо и попытался помочь раненой, выжил только потому, что у экстремиста заклинило оружие. Разочарованный невозможностью попасть в синагогу, злоумышленник решил убивать людей, похожих на мигрантов. Он поехал на арендованной машине в ближайшую кебабную лавку, где убил 20-летнего мужчину из дробовика. Затем он направился в Ландсберг, находящийся примерно в 15 км от Галле, где стал стрелять в пешеходов и ранил еще двух человек. Террорист в прямом эфире транслировал всю атаку через стриминговый сервис «Twitch», поскольку он надеялся представить ее широкой публике и побудить других единомышленников совершить аналогичные действия.*

Полицейское расследование показало, что нападавший был крайне правым экстремистом. Террористическая атака в Галле является весьма специфичной из-за использования технологии 3D-принтера,

что позволило сконструировать самодельное оружие. С помощью бесплатных интернет-справочников, доступных каждому, террорист смог распечатать оружие. Кроме того, террорист заявил, что изготовил собственное оружие, чтобы доказать, что нападение несложно реализовать с применением самодельного оружия. Части оружия, использованного при нападении в Галле, не обязательно были предназначены для этой цели.

Однако по мере того, как качество 3D-печати повышается, а технология становится все более известной и доступной, риск и эффективность террористов, производящих свое оружие, вероятно, еще больше возрастут. Это может быть первым шагом на пути к созданию прочного, напечатанного на 3D-принтере оружия для террористических атак. Если террористы уже поддерживают производство собственного огнестрельного оружия с 3D-компонентами, то это будет лишь вопросом времени, когда террористы смогут напрямую изготавливать свое собственное прочное оружие.

3D-печать металлом — это новая технология, которая также станет более распространенной. В 2013 г. одна из техасских компаний напечатала металлическую копию пистолета M1911, из которого было выпущено 600 патронов. Другой случай в Соединенных Штатах — запрет, вынесенный федеральным судьей в отношении компании «Defense Distributed», которая разрабатывает чертежи для полиграфического оружия. Компания продавала онлайн-инструкции, как печатать детали для AR-15 и другого оружия.

Люди все чаще комбинируют детали, напечатанные на 3D-принтере, с металлическими деталями для создания оружия, что, в свою очередь, увеличивает риск атак из-за их доступности.

Преступный мир уже практически поставил производство оружия на поток. В апреле 2021 г. испанская полиция заявила о том, что было обезврежено производство оружия на 3D-принтере в подпольной лаборатории в городе Санта-Крус-де-Тенерифе на Канарских островах.

Широкое распространение 3D-печати и простота передачи компьютерных файлов могут в конечном итоге повлиять на распространение ядерного оружия так, как они влияют на обычное вооружение прямо сейчас. Например, ***компания «Raytheon» печатает компоненты управляемого оружия, которое может служить элементом системы для ядерной боеголовки***. Это часть технологий будущего, когда государства будут использовать 3D-печать для разработки ядерного оружия.

Беспилотные автомобили

Еще в 2014 г. Группа по стратегическим вопросам, входящая в состав Управления разведки ФБР, прогнозировала, что «автономия [откроет пути для автомобиля], чтобы стать более потенциальным смертоносным оружием, чем сегодня».

Другой аспект данной проблемы — ***использование беспилотных автомобилей в качестве взрывных устройств***. Простые автомобили с бомбами — обычная тактика, применяемая рядом террористических организаций на протяжении последних десятилетий практически по всему миру. Примерами могут послужить использование Ирландской освободительной армией автомобильных бомб с 1970-х по 1990-е гг. или взрыв в 1993 г. Всемирного торгового центра в Нью-Йорке. Однако в последние два десятилетия автомобильные бомбы чаще всего взрывались на Ближнем Востоке, особенно в Ираке и Сирии.

Террористы уже начали использовать автоматизацию, что иллюстрирует пример разработки ИГИЛ дистанционно управляемой заминированной машины. В этом конкретном случае террористы даже поставили поддельный драйвер с термостатами, чтобы избежать обнаружения сканерами безопасности. Использование автономных и полуавтономных автомобилей было бы большим преимуществом для террористов.

Направление транспортных средств в толпу — еще одна возможность использования террористами беспилотных автомобилей. За последние годы совершено множество нападений с грузовиками, использовавшимися в качестве оружия, трагическими примерами которых были атаки в Ницце и Берлине — оба события произошли в 2016 г. В первом случае гражданин Туниса по имени Мохамед Лахуайей Бухлель намеренно врезался на 20-тонном грузовике в толпу на Английской набережной, убив 86 человек и многих ранив. Другой подобный теракт тоже был совершен тунисцем, который въехал на грузовике на рождественскую ярмарку в Берлине, убив 12 человек и ранив более 50.

Упомянутые нападения — это только два из значительного числа зарегистрированных нападений такого рода.

Если террористы воспользуются технологиями автономных транспортных средств, они могут нанести гораздо больший ущерб, особенно при его совмещении наезда со взрывом бомбы.

Кроме того, ожидается, что террористы будут вмешиваться в алгоритмы транспортных средств, чтобы те нарушали свои запрограммированные инструкции по безопасности и выезжали на тротуар

или в другие места, заполненные людьми, с целью причинить вред как можно большему их количеству.

Одним из методов, позволяющих террористам взять под контроль автономное или полуавтономное транспортное средство, помимо использования собственных запрограммированных автомобилей, может стать взлом чужого автомобиля и использование его в терактах. На сегодняшний день проведено множество «хакерских тестов», нацеленных на доказательство того, что современные автомобили — не полностью автономные, но технологически продвинутые — уязвимы для кибератак. Примером может служить эксперимент по взлому автомобиля, проведенный в 2015 г., когда хакеры взяли под контроль его систему климат-контроля, радио, лобовые стекла, а также тормоза и рулевое управление. Установление контроля над первыми тремя единицами оборудования не представляет большой опасности для водителя или других лиц, но управление тормозами и рулевое управление на дороге сопряжены с серьезными травмами и могут быть опасны для жизни.

Еще более тревожным является сценарий, когда террористы получают контроль над несколькими транспортными средствами одновременно, что дает возможность вызывать множественные аварии, в конечном итоге блокировать дороги, при одновременном проведении атаки с использованием взрывчатых материалов.

Дипфейки

Термин «глубокая подделка» используется для описания реалистичных фото, аудио, видео и других подделок, созданных с помощью технологий ИИ, он впервые был использован в 2017 г. Чаще всего глубокие подделки создаются с помощью методов машинного обучения, в частности генеративно-состязательных сетей (известных как GAN).

Дипфейки также могут представлять широкий спектр угроз для национальной и международной безопасности. Авторы исследования, проведенного в Университетском колледже Лондона в 2020 г., утверждают, что фальшивый аудио- или видеоконтент был оценен экспертами как наиболее тревожное применение ИИ с точки зрения его потенциального применения для преступлений или терроризма. Одним из примеров использования глубоких фейков в гнусных целях является публикация фальшивых видеороликов публичных деятелей, особенно политиков, в которых те демонстрируют ненадлежащее поведение, которое может подорвать доверие людей к таким лицам.

Одним из потенциальных сценариев может оказаться вариант, когда члены террористической организации используют глубокие подделки, чтобы выдать себя за чьих-то родственников или руководителей с целью извлечения средств, которые могут быть использованы для финансирования их противоправной деятельности. Террористы могут сделать это, пытаясь воспроизвести свой голос; в таких случаях они используют программу, которая клонирует голоса. В отношении инцидента, произошедшего в 2020 г., сообщалось, что киберпреступники действовали именно так: они использовали технологию ИИ, чтобы выдать себя за босса главного исполнительного директора компании, и обманом заставили его перевести на свои счета 243 тыс. долл.

Другой опасный вариант — это создание террористами реалистичного контента (фото или видео), направленного на усиление радикализации и активизацию их кампаний по вербовке. Такой фальшивый контент может, например, демонстрировать, как американские, британские или французские солдаты совершают военные преступления (избивают захваченных джихадистов или истязают их каким-либо другим способом), что не только лишит легитимности контртеррористические усилия, но и привлечет новобранцев к террористам.

Социальные сети

До эпохи социальных сетей террористические организации пытались использовать 24-часовые циклы, общенациональные или международные телевизионные новостные каналы. Вопреки непосредственным впечатлениям, отношения между террористами и СМИ были не паразитическими, а симбиотическими по своей природе. Во время террористической атаки в СМИ попадали шокирующие кадры, которые, в свою очередь, гарантировали высокую аудиторию, в то время как террористы достигали своих целей: охватить широкую общественность с помощью запланированных методов коммуникации и в результате получить известность. Однако у этой связи были некоторые ограничения, которые исчезли с ростом популярности социальных сетей, такие как цензура в основных СМИ кровавых записей, которые могут шокировать людей, а также привлекать потенциальных новобранцев. Традиционные СМИ всегда представляли террористов в явно негативной форме, а вместо этого социальные сети дали голос также и их сторонникам. Более того, они создают возможность для передачи информации в реальном времени и для охвата гораздо большей аудитории без возрастных ограничений.

Интернет и социальные сети дали два типа преимуществ.

Во-первых, они ускоряют и облегчают общение между членами террористических организаций, что позволяет им легко координировать глобальные атаки. Кроме того, они позволяют им обращаться ко всем пользователям интернета и социальных сетей с их индивидуализированным контентом.

Во-вторых, социальные сети дали террористам возможность транслировать свои атаки в режиме реального времени, а также проводить долгосрочные операции в киберпространстве, такие как пропагандистские кампании. Например, деятельность в инфосфере «Исламского государства» показала, что эта организация проводит не разовые, независимые действия, но координирует их серию, которую можно охарактеризовать как «информационную войну» в киберпространстве. Они сосредоточены не только на аспектах запугивания, но и на увеличении числа своих сторонников, привлечении новобранцев, которые стремятся прибыть в контролируемые районы, чтобы поддержать ИГИЛ в построении общественной жизни, а также проводить террористические акты самостоятельно в качестве «одиноких волков».

Пропагандистские материалы, подготовленные и опубликованные «Исламским государством», указали на некоторые способы использования террористами технологических инноваций. Уровень сложности и продвинутости этих материалов зависит от уровня организационного развития, которого террористы достигли на тот момент. Пропаганда использовалась для достижения самых разных целей: угрозы оппонентам, поощрение молодых мужчин присоединиться к боевикам ИГИЛ и молодых женщин, чтобы внести свой вклад в построение общества ИГИЛ, и, наконец, что не менее важно, мотивация людей совершать террористические атаки самостоятельно. Сбор сторонников и людей, готовых оказать военную и социальную поддержку организации, посредством производства специально подготовленных видеоматериалов и выпуска большого количества фейковых новостей или прямого общения с потенциальными новобранцами, принес террористам положительные результаты. Существует множество примеров вербовки женщин и мужчин в ряды террористов, которые обсуждались в СМИ.

Самые умелые организации были наиболее эффективными в адаптации своей медиадеятельности.

Еще один негативный пример использования террористами социальных сетей — ***пропаганда своей деятельности в режиме реального времени***. Известным примером такого негативного использования социальных сетей было нападение, совершенное в марте

2019 г. в Крайстчерче (Новая Зеландия), когда правый экстремист не менее 17 минут транслировал в прямом эфире в *Facebook* нападение, в результате которого был убит 51 человек.

Платформы социальных сетей осознают свою роль в распространении дезинформации и пропаганды террористов и, чтобы остановить это, приняли меры. В конце ноября 2019 г. в рамках совместной работы Отдела интернет-справок Европейского союза, Европола, Евроюста и онлайн-платформ значительное количество веб-сайтов и учетных записей в социальных сетях было приостановлено.

Аналогичные шаги были сделаны Институтом стратегического диалога, который в октябре 2019 г. обнаружил гигантское хранилище данных ИГИЛ. Об этом были проинформированы власти Великобритании и США.

Несмотря на многочисленные инициативы по борьбе со злонамеренными действиями в интернете, реализованные решения по-прежнему недостаточны для того, чтобы остановить террористов и преступников. Ярким примером были беспорядки в США в 2020 г., спровоцированные смертью рецидивиста Джорджа Флойда и вызванные вредоносной деятельностью третьих лиц в социальных сетях.

Меры по недопущению применения террористами новых технологий

9 декабря 2020 г. Комиссия ЕС представила пресс-релиз, в котором пообещала улучшить контртеррористические возможности блока. Основное внимание в этом обязательстве уделяется ***увеличению частоты и качества обмена разведданными между государствами-членами и Центром разведки и ситуационного анализа блока (EU INTCEN)*** для выявления будущих угроз при инвестировании в новые технологии (например, ИИ), а также борьбе с радикализацией онлайн и в тюрьмах через удаление террористического содержания. Они также заявили, что новое ***«Обязательство ЕС по безопасности и устойчивости городов»*** будет сосредоточено на обеспечении финансирования для защиты густонаселенных и символических территорий, при этом с возможностью отдельного увеличения полномочий Европола и ***программы обмена полицейской информацией***.

Динамика среды безопасности и увеличение темпов технического прогресса требуют учитывать все факторы по сдерживанию перечисленных технологических угроз. Авторы доклада из европейского института видят следующие меры по сдерживанию.

1. Из-за международных террористических угроз и возможного приобретения террористами передовых технологий жизненно важным представляется начать глобальную дискуссию о будущих проблемах, связанных с ними. Силовые структуры должны сотрудничать для предотвращения вредного использования новых технологий с негосударственными субъектами, а также для осуществления контроля того, как их разработка ведется военным или гражданским сектором, принадлежащим государствам, разрабатывающим ИИ.

2. Аналитики полиции и разведки должны сотрудничать для проверки и выявления наиболее уязвимых секторов, в которых новые технологии, особенно ИИ, могут быть использованы злонамеренно.

3. Данные исследований и разработок в сфере новых технологий должны быть максимально защищены с использованием методов кибербезопасности. Учитывая, что важность разработки таких технологий невозможно переоценить, многие участники могли бы прибегнуть к кибератакам и не только для кражи технологий. От крупных государственных субъектов до негосударственных субъектов данные ИИ будут подвергаться множеству хакерских нападений с намерением украсть их и интегрировать в собственные системы. В связи с этим вовлеченные организации вместе с силовыми структурами должны усилить ИТ-обучение персонала, а также улучшить свое антихакерское и идентификационное программное обеспечение, чтобы хакеры не могли получить легкий доступ к информации. ИИ также может оказаться грозным инструментом как для кибербезопасности, так и для кибератак, поскольку он может действовать намного быстрее, чем люди, в случае такой атаки, совершенной субъектом, или будучи объектом, подвергшимся ей.

4. Постоянное использование БПЛА на поле боя ведет к оцифровке регулярных войн. Кроме того, БПЛА можно использовать для перевозки взрывчатых веществ, оружия, наркотиков или опасных химикатов. Особое внимание полиции и разведке следует уделять двойному использованию различных технологически продвинутых инструментов, которые могут принести пользу как обычным людям, так и террористам.

5. Каждая покупка, приобретение или использование БПЛА должно быть отмечено для предоставления информации о пользователе этой конкретной машины. Это похоже на ракетные системы отдельных государств или на покупку оружия отдельными лицами,

когда пользователи и поставщики должны делиться своей информацией для использования оружия.

6. 3D-печать неизбежно станет одной из ключевых угроз государственной безопасности. Возможность создать собственное оружие дома может привести к частым столкновениям между преступниками, террористами и полицией. По этой причине необходимо ужесточить новые правила об обмене чертежами оружия в интернете, а также об их открытой продаже. Службы национальной безопасности должны сосредоточиться на наблюдении за людьми, которые ищут чертежи для 3D-печатного оружия или делятся своими знаниями о том, как создавать оружие, в социальных сетях. Одной из форм регулирования распространения чертежей является выдача утвержденных правительством сертификатов, которые позволяют доверенным компаниям продавать свои чертежи прошедшим проверку лицам. Это может быть дополнительно усилено созданием общегосударственной базы данных, которая отслеживает, кому разрешено покупать или продавать эти предметы.

Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях (проект)[1]

Содержание

Преамбула
Глава I. Общие положения
Глава II. Криминализация, уголовное производство и правоохранительная деятельность
Раздел 1. Установление ответственности
Раздел 2. Уголовное судопроизводство и правоохранительная деятельность
Глава III. Меры по противодействию преступлениям и иным противоправным деяниям в информационном пространстве
Глава IV. Международное сотрудничество
Раздел 1. Выдача, взаимная правовая помощь и сотрудничество между правоохранительными органами
Раздел 2. Меры по возвращению активов
Глава V. Техническая помощь и подготовка кадров
Глава VI. Механизмы выполнения Конвенции
Глава VII. Заключительные положения
Приложение

ПРЕАМБУЛА

Государства — участники настоящей Конвенции,

будучи убеждены в том, что информационное пространство должно строиться в строгом соответствии с основными принципами и нормами международного права, в том числе принципами уважения прав и свобод человека и принципами мирного урегулирования споров,

учитывая, что каждое государство обладает суверенитетом и осуществляет юрисдикцию в отношении информационного пространства в пределах своей территории в соответствии со своим внутренним правом,

будучи обеспокоены серьезностью порождаемых преступлениями в сфере информационно-коммуникационных технологий (ИКТ)

[1] Проект, передан Российской делегацией в специальный комитет ООН 27 июля 2021 г.

проблем и угроз для стабильности и безопасности общества, что подрывает демократические институты, ценности, справедливость и наносит ущерб устойчивому развитию и правопорядку,

будучи обеспокоены также тем, что преступное использование ИКТ создает широкие возможности для осуществления других форм преступной деятельности, включая компьютерные атаки на объекты критически важной инфраструктуры, компьютерный шпионаж, сексуальную эксплуатацию детей в сети Интернет, терроризм, мошенничество, незаконный оборот персональных данных, отмывание денежных средств,

будучи обеспокоены далее возрастающим количеством преступлений в сфере ИКТ, связанных с большими объемами активов, которые могут составлять значительную долю ресурсов государств, и ставящих под угрозу социальную, политическую стабильность и устойчивое развитие этих государств,

будучи убеждены в том, что преступления в сфере ИКТ представляют собой транснациональное явление, которое затрагивает общество и экономику всех государств, что обусловливает исключительно важное значение международного сотрудничества в области предупреждения указанных преступлений и борьбы с ними,

будучи убеждены далее в необходимости оказания технической помощи в противодействии преступлениям в сфере ИКТ, которая играет важную роль в расширении возможностей государств в области эффективного предупреждения преступлений и повышения уровня информационной безопасности,

учитывая, что предупреждение и искоренение преступлений в сфере ИКТ — это обязанность всех государств и что для обеспечения эффективности своих усилий в данной области они должны сотрудничать друг с другом при поддержке и участии государственно-частного партнерства, бизнеса, отдельных лиц и групп за пределами публичного сектора, таких как гражданское общество, поскольку общая безопасность всего информационного пространства зависит от усилий каждого государства,

будучи преисполнены решимости более эффективно предупреждать, выявлять и пресекать международные переводы незаконно приобретенных в результате совершения преступлений в сфере ИКТ активов и укреплять международное сотрудничество в принятии мер по возвращению активов,

учитывая также принципы справедливости, равенства перед законом и необходимость содействия формированию в обществе культуры, отвергающей правонарушения в сфере ИКТ,

принимая во внимание резолюцию Генеральной Ассамблеи ООН от 27 декабря 2019 г. № 74/274 «Противодействие использованию информационно-коммуникационных технологий в преступных целях», на основании которой учрежден специальный межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях,

согласились о нижеследующем:

ГЛАВА I. ОБЩИЕ ПОЛОЖЕНИЯ

Статья 1. Цели

Целями настоящей Конвенции являются:

содействие принятию и укреплению мер, направленных на эффективное предупреждение преступлений и иных противоправных деяний в сфере ИКТ и борьбу с ними;

предотвращение действий, направленных против конфиденциальности, целостности и доступности ИКТ, и предупреждение злоупотреблений в сфере использования ИКТ путем обеспечения наказуемости деяний, охватываемых настоящей Конвенцией, и предоставления полномочий, достаточных для эффективной борьбы с такими преступлениями и иными противоправными деяниями, путем содействия выявлению и расследованию таких деяний и преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей о международном сотрудничестве;

повышение эффективности и развитие международного сотрудничества, в том числе в контексте подготовки кадров и оказания технической помощи в предупреждении преступлений в сфере ИКТ и борьбе с ними.

Статья 2. Сфера применения

Настоящая Конвенция применяется в соответствии с ее положениями к предупреждению, выявлению, пресечению, расследованию и преследованию за преступления и иные противоправные деяния, признанные таковыми в соответствии со статьями 6–29 настоящей Конвенции, а также осуществлению мер по устранению последствий совершения таких деяний, включая приостановление операций, связанных с активами, приобретенными в результате совершения какого-либо из преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, арест, конфискацию и возвращение доходов от таких преступлений.

Для целей осуществления настоящей Конвенции, если в ней не предусмотрено иное, не является необходимым, чтобы в результате совершения указанных в ней преступлений и иных противоправных деяний был причинен имущественный вред.

Статья 3. Защита суверенитета

1. Государства-участники осуществляют свои обязательства согласно настоящей Конвенции в соответствии с принципами государственного суверенитета, суверенного равенства государств и невмешательства во внутренние дела других государств.

2. Настоящая Конвенция не наделяет компетентные органы Государства-участника правом осуществлять на территории другого Государства-участника юрисдикцию и функции, которые относятся к исключительной компетенции органов этого другого государства, если иное не предусмотрено в настоящей Конвенции в соответствии с его внутренним законодательством.

Статья 4. Термины и определения

Для целей настоящей Конвенции:

a) «арест имущества» означает временное запрещение передачи, преобразования, отчуждения или передвижения имущества, или временное вступление во владение таким имуществом, или временное осуществление контроля над ним по постановлению суда или другого компетентного органа;

b) «бот-сеть» означает два и более устройства ИКТ, на которые установлена вредоносная программа, управляемая централизованно и скрытно от пользователей;

c) «вредоносная программа» означает программу, объективными свойствами которой являются несанкционированные модификация, уничтожение, копирование, блокирование информации или нейтрализация средств защиты информации в цифровой форме;

d) «детская порнография» определяется в соответствии с пунктом «c» статьи 2 Факультативного протокола к Конвенции о правах ребенка, касающимся торговли детьми, детской проституции и детской порнографии, от 25 мая 2000 года;

e) «доходы» означает любое имущество, приобретенное или полученное, прямо или косвенно, в результате совершения какого-либо преступления и иного противоправного деяния, предусмотренного настоящей Конвенцией, а также прибыль или другие выгоды, которые получены от таких доходов, от имущества, в которое были превращены или преобразованы такие доходы, или от имущества, к которому были приобщены такие доходы;

f) «информационно-коммуникационные технологии» (ИКТ) означает процессы и методы создания, обработки, распространения информации, а также способы и средства их осуществления;

g) «информационно-телекоммуникационные сети» означает совокупность инженерного оборудования, предназначенного для управления технологическими процессами с применением средств вычислительной техники и телекоммуникаций;

h) «имущество» означает любые активы, материальные и нематериальные, движимые или недвижимые, выраженные в вещах или в правах, включая денежные средства, в том числе находящиеся на банковских счетах, цифровые финансовые активы, цифровую валюту, включая криптовалюту, а также юридические документы или акты, подтверждающие право на такие активы или на их часть;

i) «информация» означает любые сведения (сообщения, данные), независимо от формы их представления;

j) «конфискация» означает принудительное безвозмездное изъятие имущества на основании постановления суда или другого компетентного органа;

k) «компьютерная атака» означает целенаправленное воздействие программных и (или) программно-аппаратных средств на информационные системы или информационно-телекоммуникационные сети в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

l) «цифровая информация» означает сведения (данные), независимо от формы и характеристик, содержащиеся и обрабатываемые в информационно-телекоммуникационных устройствах, системах и сетях;

m) «критическая информационная инфраструктура» означает совокупность объектов критической информационной инфраструктуры, а также сетей электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры между собой;

n) «объекты критической инфраструктуры» означает информационные системы и информационно-коммуникационные сети государственных органов, а также информационные системы и автоматизированные системы управления технологическими процессами, функционирующие в сфере оборонной промышленности, здравоохранения, образования, транспорта, связи, энергетики, кредитно-финансовой сфере, атомной и других важных сферах жизнедеятельности государства и общества;

o) «поставщик услуг» означает:

i) любую государственную или частную организацию, которая обеспечивает пользователям ее услуг возможность обмена информацией посредством использования ИКТ, или

ii) любую другую организацию, которая осуществляет обработку или хранение информации в электронной форме от имени организации, упомянутой в подпункте (i), или пользователей услуг такой организации;

p) «технические параметры трафика» означают любую информацию в электронной форме (за исключением содержания передаваемых данных), связанную с передачей данных с использованием ИКТ и указывающую, в частности, на источник передачи данных, пункт назначения, маршрут, время, дату, размер, продолжительность, тип соответствующего сетевого сервиса;

q) «устройство ИКТ» означает совокупность (комплекс) технических средств, использующуюся/предназначенную для автоматизированной обработки, хранения и передачи информации в электронной форме;

r) «электронное доказательство» означает любую доказательную информацию, хранимую или передаваемую в цифровой форме (на электронном носителе информации).

Понятие «существенный ущерб» определяется в соответствии с внутренним законодательством запрашиваемого Государства-участника.

ГЛАВА II. КРИМИНАЛИЗАЦИЯ, УГОЛОВНОЕ ПРОИЗВОДСТВО И ПРАВООХРАНИТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

Раздел 1. УСТАНОВЛЕНИЕ ОТВЕТСТВЕННОСТИ

Статья 5. Установление ответственности

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству деяний, предусмотренных как минимум статьями 6, 7, 9–12, 14–17, 19–20, 22–26, 28 настоящей Конвенции, применяя при этом такие уголовные и иные санкции, включая лишение свободы, которые учитывают степень общественной опасности конкретного деяния и размер причиненного ущерба.

Статья 6. Неправомерный доступ к цифровой информации

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленного неправомерного доступа к цифровой информации,

повлекшего ее уничтожение, блокирование, модификацию либо копирование.

Статья 7. Неправомерный перехват

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленного перехвата цифровой информации, осуществляемого без соответствующих прав и (или) с нарушением установленных норм, в том числе с использованием технических средств перехвата технических параметров трафика и данных, обрабатываемых с использованием ИКТ и не предназначенных для общего пользования.

Статья 8. Неправомерное воздействие на цифровую информацию

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству умышленного неправомерного воздействия на цифровую информацию путем ее повреждения, удаления, изменения, блокирования, модификации либо копирования информации в цифровой форме.

Статья 9. Нарушение функционирования информационно-коммуникационных сетей

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленного неправомерного действия, направленного на нарушение функционирования информационно-коммуникационных сетей, повлекшего тяжкие последствия или создавшего угрозу их наступления.

Статья 10. Создание, использование и распространение вредоносных программ

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленных создания, в том числе адаптирования, использования и распространения вредоносных программ, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования, распространения цифровой информации или нейтрализации средств ее защиты, за исключением случаев правомерного проведения исследований.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в ка-

честве преступления или иного противоправного деяния, согласно его внутреннему законодательству, создания или использования бот-сети для целей совершения какого-либо из деяний, предусмотренных положениями статей 6–12, 14 настоящей Конвенции.

Статья 11. Неправомерное воздействие на критическую информационную инфраструктуру

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству умышленных создания, распространения и (или) использования компьютерных программ либо иной цифровой информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству нарушения правил эксплуатации средств хранения, обработки и передачи охраняемой цифровой информации, содержащейся в критической информационной инфраструктуре, или информационных систем, информационно-коммуникационных сетей, относящихся к критической информационной инфраструктуре, либо правил доступа к ним, если оно повлекло причинение вреда критической информационной инфраструктуре.

Статья 12. Несанкционированный доступ к персональным данным

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания согласно его внутреннему законодательству в качестве преступления несанкционированного доступа к персональным данным в целях их уничтожения, изменения, копирования, распространения.

Статья 13. Незаконный оборот устройств

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству незаконных производства, продажи, приобретения для использования, импорта, экспорта или иных форм предоставления в пользование устройств, разработанных или адаптированных прежде всего для целей совершения какого-либо из преступлений, предусмотренных положениями статей 6–12 настоящей Конвенции.

Положения настоящей статьи не распространяются на случаи, когда производство, продажа, приобретение для использования, импорт, экспорт или иные формы предоставления в пользование устройств связаны, например, с разрешенным испытанием или защитой компьютерной системы.

Статья 14. Хищение с использованием ИКТ

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству хищения имущества либо незаконного приобретения права на него, в том числе посредством мошенничества, путем уничтожения, блокирования, модификации либо копирования цифровой информации или иного вмешательства в функционирование ИКТ.

2. Каждое Государство-участник может оставить за собой право считать хищение имущества либо незаконное приобретение права на него, в том числе посредством мошенничества, с использованием ИКТ признаком, отягчающим наказание при совершении хищения в формах, определенных внутренним законодательством.

Статья 15. Преступления, связанные с изготовлением и оборотом материалов или предметов с порнографическими изображениями несовершеннолетних, совершенные с использованием ИКТ

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству в случае совершения умышленно и неправомерно следующих деяний:

a) производство детской порнографической продукции в целях распространения через информационно-коммуникационные сети, включая сеть Интернет;

b) предложение или предоставление в пользование детской порнографии через информационно-коммуникационные сети, включая сеть Интернет;

c) распространение, передача, публичная демонстрация или рекламирование детской порнографии с использованием информационно-коммуникационных сетей, включая сеть Интернет;

d) приобретение детской порнографии посредством использования ИКТ для себя или для другого лица;

e) владение детской порнографией, находящейся в компьютерной системе или на электронно-цифровых носителях информации.

2. Для целей пункта 1 настоящей статьи в понятие «детская порнография» включаются порнографические материалы, изображающие:

a) участие несовершеннолетнего лица в откровенных сексуальных действиях;

b) участие лица, кажущегося несовершеннолетним, в откровенных сексуальных действиях;

c) реалистические изображения несовершеннолетнего лица, участвующего в откровенных сексуальных действиях.

Для целей настоящей статьи термин «несовершеннолетние» означает любое лицо, не достигшее 18-летнего возраста. Однако любая Сторона может устанавливать и более низкие возрастные пределы, но не ниже 16 лет.

Статья 16. Склонение к самоубийству или доведение до его совершения

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству склонения к самоубийству или доведения до самоубийства, в том числе несовершеннолетних, совершенных посредством оказания психологического и иных видов воздействия в информационно-телекоммуникационных сетях, включая сеть Интернет.

Статья 17. Преступления, связанные с вовлечением несовершеннолетнего в совершение противоправных действий, опасных для его жизни и здоровья

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству вовлечения несовершеннолетнего посредством использования ИКТ в совершение противоправных деяний, представляющих опасность для его жизни, за исключением действий, предусмотренных статьей 16 настоящей Конвенции.

Статья 18. Создание и использование цифровой информации для введения пользователя в заблуждение

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству умышленного противоправного создания и использования цифровой информации, сходной до степени смешения с уже известной пользователю и вызывающей доверие информацией, повлекших причинение существенного ущерба.

2. Каждое Государство-участник может оставить за собой право считать такие деяния преступными, если они совершены в совокупности с иными преступлениями, предусмотренными внутренним законодательством такого Государства-участника, или содержали умысел совершения указанных преступлений.

Статья 19. Подстрекательство к подрывной или вооруженной деятельности

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенных с использованием ИКТ призывов к проведению подрывных или вооруженных действий, направленных на насильственное изменение государственного строя другого государства.

Статья 20. Преступления, связанные с террористической деятельностью

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенных с использованием ИКТ призывов к осуществлению террористической деятельности, склонения, вербовки или иного вовлечения в нее, пропаганды и оправдания терроризма, сбора или предоставления средств для целей его финансирования.

Статья 21. Преступления, связанные с экстремистской деятельностью

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству распространения материалов, содержащих призывы к совершению противоправных деяний по мотивам политической, идеологической, социальной, расовой, национальной или религиозной ненависти и вражды, пропаганды или оправдания таких деяний, либо обеспечения доступа к ним, совершенных с использованием ИКТ.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству унижения лица или группы лиц по признакам расы, национальности, языка, происхождения, отношения к религии, совершенных с использованием ИКТ.

Статья 22. Преступления, связанные с распространением наркотических средств и психотропных веществ

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в ка-

честве преступления согласно его внутреннему законодательству совершенного умышленно, посредством использования ИКТ незаконного оборота наркотических средств и психотропных веществ, а также материалов, необходимых для их изготовления.

Статья 23. Преступления, связанные с незаконным оборотом оружия

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенного умышленно, посредством использования ИКТ незаконного оборота оружия, боеприпасов, взрывных устройств и взрывчатых веществ.

Статья 24. Реабилитация нацизма, оправдание геноцида или преступлений против мира и человечности

Каждое государство принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенного с использованием ИКТ умышленного распространения материалов, в которых отрицаются факты, одобряются или оправдываются действия, являющиеся геноцидом или преступлениями против мира и человечности, установленные приговором Международного военного трибунала, образованного в соответствии с Лондонским соглашением от 8 августа 1945 года.

Статья 25. Незаконное распространение фальсифицированных лекарственных средств и медицинских изделий

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству совершенного умышленно посредством использования ИКТ незаконного распространения фальсифицированных лекарственных средств и медицинских изделий.

Статья 26. Использование ИКТ для совершения деяний, признанных преступлениями в соответствии с международным правом

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления согласно его внутреннему законодательству использования ИКТ с целью совершения какого-либо деяния, представляющего собой преступление, охватываемого каким-либо международным договором из перечисленных в Приложении к настоящей Конвенции.

2. При сдаче на хранение своих ратификационных грамот или документов о принятии, утверждении или присоединении государство, не являющееся участником какого-либо из договоров, перечисленных в Приложении к настоящей Конвенции, может заявить, что при применении настоящей Конвенции к этому Государству-участнику считается, что этот договор не включен в упомянутое Приложение. Такое заявление перестает действовать, как только этот договор вступает в силу для данного Государства-участника, которое уведомляет об этом факте депозитария.

3. Когда Государство-участник перестает быть стороной какого-либо из договоров, перечисленных в Приложении к настоящей Конвенции, оно может сделать заявление в отношении этого договора (договоров), как это предусматривается в пункте 2 настоящей статьи.

Статья 27. Нарушение авторских и смежных прав с использованием ИКТ

Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления или иного противоправного деяния согласно его внутреннему законодательству нарушения авторских и смежных прав, как они определены в законодательстве этого Государства-участника, когда такие деяния совершаются умышленно с использованием ИКТ, включая незаконное использование программ для компьютерных систем и баз данных, являющихся объектами авторского права, и присвоение авторства.

Статья 28. Соучастие в преступлении, приготовление к преступлению и покушение на преступление

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для признания в качестве преступления в соответствии со своим внутренним законодательством приготовления и покушения на какое-либо преступление, признанное таковым в соответствии с положениями настоящей Конвенции.

2. Каждое Государство-участник рассматривает возможность принятия таких законодательных и иных мер, которые необходимы для признания в качестве преступления в соответствии со своим внутренним законодательством изготовления или приспособления лицом орудий и иных средств совершения преступления, вербовки соучастников преступления, сговора на совершение преступления либо иного умышленного создания условий для совершения преступления, предусмотренного настоящей Конвенцией, если при

этом преступление не было доведено до конца по независящим от этого лица обстоятельствам.

3. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы согласно его внутреннему законодательству для установления ответственности, наряду с непосредственными исполнителями какого-либо преступления, признанного таковым в соответствии с настоящей Конвенцией, в отношении участвующих в его совершении организатора, подстрекателя или пособника, а также усиления ответственности за групповые преступления, включая организованные группы и преступные сообщества.

Статья 29. Иные противоправные деяния

Настоящая Конвенция не является препятствием для признания Государством-участником в качестве преступления любого другого противоправного деяния, совершенного умышленно с использованием ИКТ и повлекшего существенный ущерб.

Статья 30. Ответственность юридических лиц

1. Каждое Государство-участник принимает такие законодательные и иные правовые меры, которые необходимы для обеспечения возможности привлечения к ответственности юридических лиц в связи с преступлениями и иными противоправными деяниями, признанными в качестве таковых в соответствии с настоящей Конвенцией, если эти деяния совершены в их интересах любым физическим лицом, действующим в личном качестве или в качестве члена органа соответствующего юридического лица, занимающего в данном юридическом лице руководящую должность на основании:

a) полномочий представлять данное юридическое лицо;

b) права принимать решения от имени этого юридического лица;

c) права осуществлять контроль внутри этого юридического лица.

2. В дополнение к случаям, предусмотренным пунктом 1 настоящей статьи, каждое Государство-участник принимает меры, необходимые для обеспечения возможности возложения ответственности на юридическое лицо в случаях, когда отсутствие руководства или контроля со стороны физического лица, упомянутого в пункте 1, делает возможным совершение преступления или иного противоправного деяния, предусмотренного положениями настоящей Конвенции, в пользу этого юридического лица физическим лицом, действующим на основании данных ему полномочий.

3. В зависимости от правовых принципов Государства-участника ответственность юридического лица может быть уголовной, гра-

жданско-правовой или административной. Государство-участник обеспечивает применение в отношении юридических лиц, привлекаемых к ответственности, эффективных, соразмерных и оказывающих сдерживающее воздействие санкций, включая финансовые.

4. Привлечение к ответственности юридических лиц не исключает привлечения к ответственности физических лиц, совершивших преступление и иное противоправное деяние.

Раздел 2. УГОЛОВНОЕ СУДОПРОИЗВОДСТВО И ПРАВООХРАНИТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ

Статья 31. Сфера применения процессуальных норм

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые необходимы для установления полномочий и процедур, предусмотренных положениями настоящего раздела, в целях предупреждения, выявления, пресечения, раскрытия и расследования преступлений и иных противоправных деяний и осуществления судебного разбирательства в связи с ними.

2. За исключением случаев, когда положениями статьи 33 настоящей Конвенции предусматривается иное, каждое Государство-участник применяет полномочия и процедуры, упомянутые в пункте 1 настоящей статьи, в отношении:

a) преступлений и иных противоправных деяний, предусмотренных статьями 6–29 настоящей Конвенции;

b) других преступлений и иных противоправных деяний, совершенных с использованием ИКТ;

c) сбора доказательств, в том числе электронных, совершения преступлений и иных противоправных деяний.

3. a) Каждое Государство-участник может сделать оговорку о сохранении за собой права применять меры, предусмотренные статьей 38 настоящей Конвенции, только в отношении преступлений или категорий преступлений, указанных в этой оговорке, при условии, что круг таких преступлений или категорий преступлений не более ограничен, чем круг преступлений, к которым оно применяет меры, предусмотренные статьей 33 настоящей Конвенции. Каждое Государство-участник рассматривает возможность ограничения сферы действия такой оговорки с целью максимально широкого применения мер, предусмотренных положением статьи 38 настоящей Конвенции;

b) в том случае, когда Государство-участник ввиду ограничений, предусмотренных внутренним законодательством, действующим на момент принятия настоящей Конвенции, не имеет возможности применить меры, предусмотренные статьями 33 и 38 настоящей Кон-

венции, к информации, передаваемой по информационной системе поставщика услуг, которая:

i) используется для обслуживания отдельной группы пользователей и

ii) не использует информационно-телекоммуникационную сеть, а также не соединена ни с какими другими информационными системами,

это Государство-участник может сохранить за собой право не применять указанные меры к такой передаче информации.

Статья 32. Условия и гарантии

1. Каждое Государство-участник обеспечивает, чтобы установление, исполнение и применение полномочий и процедур, предусмотренных настоящим разделом, осуществлялись в соответствии с условиями и гарантиями, предусмотренными нормами его внутреннего законодательства, обеспечивающими надлежащую защиту прав и свобод человека, включая права, вытекающие из обязательств, которые Государство-участник взяло на себя по Международному пакту о гражданских и политических правах от 16 декабря 1966 года и по другим применимым международным договорам по правам человека.

2. Такие условия и гарантии с учетом характера полномочий и процедур включают, среди прочего, судебный или иной независимый надзор, основания правомочности применения, ограничения сферы и сроков действия таких полномочий или процедур.

3. В той мере, в какой это соответствует публичным интересам, в частности осуществлению правосудия, Государство-участник рассматривает влияние предусмотренных данным разделом полномочий и процедур на права, законные интересы и ответственность третьих лиц.

Статья 33. Сбор информации, передаваемой с использованием ИКТ

1. Каждое Государство-участник принимает такие законодательные и иные меры в целях противодействия преступлениям, предусмотренным настоящей Конвенцией и признанным таковыми в соответствии с его внутренним законодательством, какие могут быть необходимы для того, чтобы наделить его компетентные органы полномочиями:

a) собирать или записывать с применением технических средств информацию, передаваемую с использованием ИКТ, на территории этого Государства-участника, и

b) обязать поставщика услуг в пределах имеющихся у него технических возможностей:

i) собирать или записывать с использованием технических средств на территории этого Государства-участника информацию в электронной форме, включающую данные о содержании сообщений, передаваемую с использованием ИКТ, или

ii) сотрудничать с компетентными органами этого Государства-участника и помогать им в сборе или записи в режиме реального времени информации в электронной форме, включающей данные о содержании сообщений, передаваемой с использованием ИКТ, на территории этого Государства-участника.

2. Если какое-либо Государство-участник в силу устоявшихся принципов его системы внутреннего права не может принять меры, предусмотренные в пункте 1 (a) настоящей статьи, то вместо этого оно может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени информации в электронной форме, включающей данные о содержании сообщений, передаваемой с использованием ИКТ на его территории, путем применения технических средств на этой территории.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий и действий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 34. Оперативное обеспечение сохранности накопленной информации в электронной форме

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы его компетентные органы имели возможность отдавать соответствующие распоряжения или указания или схожим образом оперативно обеспечивать сохранность конкретной электронно-цифровой информации, включая технические параметры трафика, в частности в случаях, когда имеются основания полагать, что эти данные особенно подвержены риску уничтожения, блокирования, копирования или модификации, в том числе в результате истечения срока давности их хранения, установленного внутренним законодательством или правилами предоставления услуг провайдера.

2. Если Государство-участник реализует положения пункта 1 настоящей статьи посредством дачи распоряжения какому-либо лицу (в том числе юридическому) об обеспечении сохранности

конкретной хранимой информации, находящейся во владении или под контролем этого лица, то это Государство-участник принимает такие законодательные и иные правовые меры, какие могут потребоваться для того, чтобы обязать это лицо хранить эту информацию и обеспечивать ее целостность в течение необходимого периода времени, но не превышающего такого срока, установленного внутренним законодательством этого государства-участника, с тем чтобы компетентные органы могли добиться раскрытия этих данных. Государство-участник может предусмотреть возможность продления срока действия такого распоряжения.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать лицо, на которое возложена обязанность по обеспечению сохранности информации, соблюдать конфиденциальность выполнения таких процедур в течение срока, предусмотренного его внутренним законодательством.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 35. Оперативное обеспечение сохранности и частичное раскрытие данных о технических параметрах трафика

1. Каждое Государство-участник принимает в отношении технических параметров трафика, сохранность которых должна быть обеспечена в соответствии с положениями статьи 34 настоящей Конвенции, такие законодательные и иные меры, какие могут быть необходимы для того, чтобы:

a) гарантировать, чтобы такое оперативное обеспечение сохранности технических параметров трафика было возможным независимо от того, сколько поставщиков услуг были вовлечены в передачу данной информации, и

b) гарантировать оперативное раскрытие компетентным органам этого Государства-участника достаточного количества технических параметров трафика, которое позволит соответствующему Государству-участнику идентифицировать поставщиков услуг и путь, которым передавалась указанная информация.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 36. Распоряжение о предоставлении информации

1. В целях, предусмотренных пунктом 1 статьи 31 настоящей Конвенции, каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того,

чтобы предоставить своим компетентным органам полномочия отдавать распоряжения:

a) лицу на территории этого Государства-участника о предоставлении конкретной электронно-цифровой информации, находящейся во владении или под контролем этого лица;

b) поставщику услуг, предлагающему свои услуги на территории этого Государства-участника, о предоставлении находящихся во владении или под контролем этого поставщика услуг сведений о его абонентах.

2. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

3. Для целей настоящей статьи термин «сведения об абонентах» означает любую имеющуюся у поставщика услуг информацию о его абонентах, кроме технических параметров трафика или содержания информации, с помощью которых можно определить:

a) вид используемой информационно-коммуникационной услуги, принятые с этой целью меры технического обеспечения и период оказания услуги;

b) личность пользователя, его почтовый или иные адреса, номера телефонов и других средств связи, включая IP-адреса, сведения о выставленных ему счетах и произведенных им платежах в рамках соглашения или договора на обслуживание;

c) сведения о месте установки информационно-коммуникационного оборудования, имеющего отношение к соглашению или договору на его обслуживание.

Статья 37. Обыск и выемка информации, хранимой или обрабатываемой в электронной форме

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут потребоваться для предоставления его компетентным органам полномочий на обыск в целях получения доступа к находящимся на территории этого Государства-участника или под его юрисдикцией:

a) устройствам ИКТ и хранящейся на них информации и

b) носителям информации, на которых может храниться искомая электронно-цифровая информация.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для обеспечения того, чтобы в случае, когда его компетентные органы в ходе обыска, производимого в соответствии с положениями пункта 1 (a) настоящей статьи, выясняют, что искомая информация хранится на другом устройстве ИКТ на территории этого Государства-участ-

ника, такие органы имели возможность оперативно произвести обыск в целях получения доступа к этому другому устройству ИКТ или содержащимся в нем данным.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий производить выемку на территории либо под юрисдикцией Государства-участника информации в электронной форме или иным аналогичным образом обеспечивать ее сохранность. Эти меры должны включать, в частности, предоставление следующих полномочий:

a) производить выемку устройств ИКТ, используемых для хранения информации, либо иным образом обеспечивать их сохранность;

b) изготавливать и сохранять копии соответствующей информации в электронно-цифровой форме;

c) обеспечивать целостность относящейся к делу хранимой информации;

d) изымать информацию, хранящуюся или обрабатываемую в электронно-цифровой форме на устройстве ИКТ.

4. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для предоставления его компетентным органам полномочий привлекать в порядке, установленном его внутренним законодательством, любое лицо, обладающее специальными знаниями о функционировании соответствующей информационной системы, информационно-телекоммуникационной сети или их частей, или применяемых мерах защиты информации, для предоставления необходимых сведений и (или) оказания содействия в осуществлении действий, предусмотренных пунктами 1–3 настоящей статьи.

5. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 38. Сбор в режиме реального времени технических параметров трафика

1. Каждое Государство-участник принимает такие законодательные и иные меры, которые могут быть необходимы для предоставления его компетентным органам полномочий:

a) собирать или записывать с применением технических средств технические параметры трафика, передаваемого с использованием ИКТ, на территории этого Государства-участника, и

b) обязать поставщиков услуг в пределах имеющихся у них технических возможностей:

i) собирать или записывать с применением технических средств на территории этого Государства-участника технические параметры трафика или

ii) сотрудничать с компетентными органами этого Государства-участника и помогать им собирать или записывать в режиме реального времени технические параметры трафика, связанные с конкретной информацией, на территории этого Государства-участника.

2. Если какое-либо Государство-участник в силу устоявшихся принципов его системы внутреннего законодательства не может принять меры, предусмотренные в пункте 1 (a) настоящей статьи, то вместо этого оно может принять законодательные и иные меры, какие могут быть необходимы для обеспечения сбора или записи в режиме реального времени технических параметров трафика на его территории путем применения технических средств на этой территории.

3. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы обязать поставщика услуг соблюдать конфиденциальность факта осуществления любых полномочий, предусмотренных в настоящей статье, и любой информации об этом.

4. Полномочия и процедуры, упомянутые в настоящей статье, устанавливаются в соответствии с положениями статей 31 и 32 настоящей Конвенции.

Статья 39. Юрисдикция

1. Каждое Государство-участник принимает такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, когда они совершены на:

a) территории этого Государства-участника, или

b) борту судна, которое несло флаг этого Государства-участника в момент совершения деяния, или воздушного судна, которое зарегистрировано в соответствии с законодательством этого Государства-участника в такой момент.

2. При условии соблюдения статьи 3 настоящей Конвенции Государство-участник может также установить свою юрисдикцию в отношении любого такого преступления и иного противоправного деяния, когда:

a) деяние совершено против гражданина этого Государства-участника, лица без гражданства, постоянно проживающего на его территории, юридического лица, учрежденного или имеющего постоянное представительство на его территории, государственного

или правительственного объекта, включая помещения дипломатического представительства и консульского учреждения этого Государства-участника; или

b) деяние совершено гражданином этого Государства-участника или лицом без гражданства, которое обычно проживает на его территории; или

c) деяние совершено против этого Государства-участника; или

d) деяние совершено полностью или частично за пределами территории Государства-участника, но его последствия составляют на его территории преступление или приводят к совершению преступления.

3. Для целей статьи 47 настоящей Конвенции каждое Государство-участник принимает такие меры, какие могут потребоваться, с тем чтобы установить свою юрисдикцию в отношении преступлений, признанных таковыми в соответствии с настоящей Конвенцией, когда лицо, подозреваемое в совершении преступления, находится на его территории и оно не выдает такое лицо на том основании, что это лицо является его гражданином либо лицом, которому этим Государством-участником предоставлен статус беженца.

4. Каждое Государство-участник, на территории которого находится лицо, подозреваемое в совершении преступления, и которое не выдает его, обязано, в случаях, предусмотренных в пунктах 1 и 2 настоящей статьи, без каких бы то ни было исключений и независимо от того, совершено ли оно на территории этого Государства-участника, без излишних задержек передать дело своим компетентным органам для целей преследования путем проведения разбирательства в соответствии с законодательством этого государства.

5. Если Государство-участник, осуществляющее свою юрисдикцию согласно пункту 1 или 2 настоящей статьи, получает уведомление или иным образом узнает о том, что любые другие Государства-участники осуществляют расследование, уголовное преследование или судебное разбирательство в связи с тем же деянием, компетентные органы этих Государств-участников проводят в надлежащих случаях консультации друг с другом с целью координации своих действий.

6. Без ущерба для норм общего международного права настоящая Конвенция не исключает осуществления любой уголовной и административной юрисдикции, установленной Государством-участником в соответствии со своим внутренним законодательством.

ГЛАВА III. МЕРЫ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПЛЕНИЯМ И ИНЫМ ПРОТИВОПРАВНЫМ ДЕЯНИЯМ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Статья 40. Политика и практика предупреждения преступлений и иных противоправных деяний в сфере использования ИКТ и борьбы с ними

1. Каждое Государство-участник в соответствии с основополагающими принципами своей правовой системы разрабатывает и осуществляет или проводит эффективную и скоординированную политику противодействия преступлениям и иным противоправным деяниям в сфере использования ИКТ.

2. Каждое Государство-участник стремится разрабатывать и поощрять эффективные виды практики, направленные на предупреждение преступлений и иных противоправных деяний в сфере использования ИКТ.

3. Государства-участники, в надлежащих случаях в соответствии с основополагающими принципами своих правовых систем, взаимодействуют друг с другом и с соответствующими международными и региональными организациями в разработке мер, указанных в настоящей статье, и содействии их осуществлению.

Статья 41. Органы по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ и борьбе с ними

1. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для того, чтобы определить органы, ответственные за осуществление деятельности по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ и борьбе с ними, и порядок взаимодействия этих органов между собой.

2. Каждое Государство-участник сообщает Генеральному секретарю Организации Объединенных Наций наименование и адрес органа или органов, которые могут оказывать другим Государствам-участникам содействие в разработке и осуществлении конкретных мер по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ.

Статья 42. Частный сектор

1. Каждое Государство-участник принимает меры в соответствии с основополагающими принципами своего внутреннего законодательства по предупреждению преступлений и иных противоправных деяний в сфере использования ИКТ в частном секторе, усилению стандартов информационной безопасности в частном секторе и в надлежащих случаях по установлению и применению

эффективных, соразмерных и оказывающих сдерживающее воздействие гражданско-правовых, административных или уголовных санкций за несоблюдение таких мер.

2. Меры, направленные на достижение этих целей, могут включать, среди прочего, следующее:

a) содействие сотрудничеству между правоохранительными органами Государства-участника и соответствующими частными организациями данного Государства-участника;

b) содействие разработке стандартов и процедур, предназначенных для обеспечения информационной безопасности;

c) содействие в обучении представителей правоохранительных, следственных, судебных органов и органов прокуратуры в сфере использования ИКТ.

Статья 43. Принципы и стандарты поведения частных организаций, предоставляющих информационно-телекоммуникационные услуги

1. Каждая частная организация (или их объединение), предоставляющая информационно-телекоммуникационные услуги, находящаяся на территории Государства-участника, принимает надлежащие меры в пределах своих возможностей и в соответствии с нормами внутреннего права этого государства для содействия формулированию и реализации принципов и стандартов функционирования международного информационного пространства на основе соблюдения прав человека, закрепленных в основополагающих документах Организации Объединенных Наций.

2. Меры, направленные на достижение этих целей, могут включать, среди прочего, следующее:

a) сотрудничество между частными организациями, предоставляющими информационно-телекоммуникационные услуги, и их объединениями;

b) сотрудничество в разработке принципов и стандартов, предназначенных для создания подходящей среды для цивилизованного общества как неотъемлемой части международного информационного пространства.

Статья 44. Повышение информированности общества в сфере предупреждения информационной преступности

1. Каждое Государство-участник принимает надлежащие меры в пределах своих возможностей и в соответствии с основополагающими принципами своего внутреннего права для содействия активному участию общественных организаций в предупреждении преступлений и иных противоправных деяний в сфере использования ИКТ и для углубления понимания обществом факта су-

ществования, причин и опасного характера этих преступлений, а также создаваемых ими угроз. Это участие следует укреплять с помощью таких мер, как:

a) обеспечение для населения эффективного доступа к информации;

b) проведение мероприятий по информированию населения, способствующих созданию атмосферы нетерпимости в отношении преступлений и иных противоправных деяний в сфере использования ИКТ, а также с целью распространения передового опыта;

c) осуществление программ публичного образования в области обеспечения безопасности ИКТ.

2. Каждое Государство-участник принимает надлежащие меры для обеспечения того, чтобы соответствующие органы по противодействию преступлениям и иным противоправным деяниям в сфере использования ИКТ, о которых говорится в настоящей Конвенции, были известны населению, и обеспечивает доступ к таким органам для предоставления им сообщений о любых случаях, которые могут рассматриваться в качестве преступлений и иных противоправных деяний в соответствии с настоящей Конвенцией.

Статья 45. Меры по защите свидетелей

Каждое Государство-участник рассматривает возможность принятия таких законодательных мер, которые могут быть необходимы для обеспечения эффективной защиты:

a) лиц, которые добросовестно и на разумных основаниях предоставляют информацию, касающуюся противоправных деяний, предусмотренных статьями 6–28 настоящей Конвенции, или иным образом сотрудничают со следственными или судебными органами;

b) свидетелей, дающих показания в отношении противоправных деяний, предусмотренных статьями 6–28 настоящей Конвенции, а также потерпевших;

c) при необходимости членов семей лиц, указанных в пунктах «a» и «b» настоящей статьи.

ГЛАВА IV. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО

Раздел 1. ВЫДАЧА, ВЗАИМНАЯ ПРАВОВАЯ ПОМОЩЬ И СОТРУДНИЧЕСТВО МЕЖДУ ПРАВООХРАНИТЕЛЬНЫМИ ОРГАНАМИ

Статья 46. Общие принципы международного сотрудничества

1. Государства-участники осуществляют максимально широкое сотрудничество в соответствии с положениями настоящей главы и путем применения других международных договоров о между-

народном сотрудничестве по уголовным делам, согласованных договоренностей, основанных на принципе взаимности, а также норм внутреннего законодательства в целях предупреждения, пресечения, выявления, раскрытия и расследования преступлений в сфере использования ИКТ.

2. Когда применительно к вопросам международного сотрудничества требуется соблюдение принципа обоюдного признания соответствующего деяния преступлением, этот принцип считается соблюденным независимо от того, включает ли законодательство запрашиваемого государства-участника соответствующее деяние в ту же категорию преступлений или описывает ли оно его с помощью таких же терминов, как запрашивающее государство-участник, если деяние, образующее состав преступления, в связи с которым запрашивается помощь, признано уголовно наказуемым в соответствии с законодательством обоих государств-участников.

3. Когда это целесообразно и соответствует их внутренней правовой системе, государства-участники оказывают друг другу содействие в расследовании и производстве по гражданско-правовым и административным делам, связанным с противоправными деяниями в сфере использования ИКТ.

4. Ни одно из преступлений, указанных в статьях 6–28 настоящей Конвенции, не рассматривается для целей выдачи и взаимной правовой помощи по уголовным делам, в том числе конфискации и возврата имущества, полученного преступным путем, между государствами-участниками как политическое преступление, преступление, связанное с политическим преступлением, или преступление, совершенное по политическим мотивам. В силу этого запрос о выдаче и оказании правовой помощи по уголовным делам, в том числе по вопросам розыска, ареста, конфискации и возврата имущества, полученного преступным путем, в связи с подобным преступлением не может быть отклонен только на том основании, что она касается политического преступления или преступления, связанного с политическим преступлением, или преступления, совершенного по политическим мотивам.

При направлении запросов и ответов на них в рамках настоящей Конвенции в экстренных случаях и при достижении договоренности между запрашивающим и запрашиваемым Государствами-участниками могут быть использованы каналы Международной организации уголовной полиции — Интерпола.

5. Каждое Государство-участник имеет равное право на защиту информационных ресурсов и критических информационных инфраструктур своего государства от неправомерного использования

и несанкционированного вмешательства, в том числе от компьютерных атак на них.

Статья 47. Выдача

1. Настоящая статья применяется к преступлениям, признанным таковыми в соответствии с настоящей Конвенцией, если лицо, выдача которого запрашивается, находится на территории запрашиваемого Государства-участника, при условии, что деяние, в связи с которым запрашивается выдача, является уголовно наказуемым по внутреннему законодательству как запрашивающего Государства-участника, так и запрашиваемого Государства-участника, при условии, что согласно внутреннему праву законодательством обоих заинтересованных Государств-участников за совершение этого деяния предусматривается наказание в виде лишения свободы на срок не менее одного года или более суровое наказание.

2. Преступления, предусмотренные статьями 6–28 настоящей Конвенции, считаются включенными в любой существующий между Государствами-участниками договор о выдаче в качестве преступлений, которые могут повлечь выдачу. Государства-участники обязуются включать такие преступления в качестве преступлений, которые могут повлечь выдачу, в любой договор о выдаче, который будет заключен между ними. Государство-участник, внутреннее законодательство которого допускает это, в случае когда оно использует настоящую Конвенцию в качестве основания для выдачи, не считает любое из преступлений, признанных таковыми в соответствии с настоящей Конвенцией, политическим преступлением.

3. Если запрос о выдаче касается нескольких отдельных преступлений, по меньшей мере одно из которых может повлечь за собой выдачу согласно настоящей статье, а другие не могут повлечь выдачу по причине срока наказания за них, но относятся к преступлениям, признанным таковыми в соответствии с настоящей Конвенцией, запрашиваемое Государство-участник может применить настоящую статью также в отношении этих преступлений.

4. Если Государство-участник, обусловливающее выдачу наличием договора, получает просьбу о выдаче от другого Государства-участника, с которым оно не имеет договора о выдаче, оно может рассматривать настоящую Конвенцию в качестве правового основания для выдачи в связи с любым преступлением, к которому применяется настоящая статья.

5. Государство-участник, обусловливающее выдачу наличием договора:

a) при сдаче на хранение своей ратификационной грамоты или документа о принятии или утверждении настоящей Конвенции или присоединении к ней сообщает Генеральному секретарю Организации Объединенных Наций о том, будет ли оно использовать настоящую Конвенцию в качестве правового основания для сотрудничества в вопросах выдачи с другими Государствами — участниками настоящей Конвенции; и

b) если оно не использует настоящую Конвенцию в качестве правового основания для сотрудничества в вопросах выдачи, стремится в надлежащих случаях к заключению договоров о выдаче с другими Государствами — участниками настоящей Конвенции в целях применения настоящей статьи.

6. Государства-участники, не обусловливающие выдачу наличием договора, в отношениях между собой признают преступления, к которым применяется настоящая статья, в качестве преступлений, которые могут повлечь выдачу.

7. Выдача осуществляется в соответствии с условиями, предусматриваемыми внутренним законодательством запрашиваемого Государства-участника, или применимыми договорами о выдаче, включая, среди прочего, условия, связанные с требованиями о минимальном наказании применительно к выдаче, и основания, на которых запрашиваемое Государство-участник может отказать в выдаче.

8. В отношении любого преступления, к которому применяется настоящая статья, Государства-участники, при условии соблюдения своего внутреннего законодательства, прилагают усилия к тому, чтобы ускорить процедуры выдачи и упростить связанные с ней требования о предоставлении доказательств, если таковые имеются.

9. Запрашиваемое государство-участник может отказать в выдаче лица, если такая выдача может нанести ущерб его суверенитету, безопасности, общественному порядку или другим существенно важным интересам.

10. При условии соблюдения положений своего внутреннего законодательства и своих договоров о выдаче запрашиваемое Государство-участник, убедившись в том, что обстоятельства требуют этого и носят неотложный характер, и по просьбе запрашивающего Государства-участника, может взять под стражу находящееся на его территории лицо, выдача которого запрашивается, или принять другие надлежащие меры для обеспечения его присутствия в ходе процедуры выдачи, включая передачу выданного лица запрашивающему Государству-участнику.

11. Государство-участник, на территории которого находится лицо, подозреваемое в совершении преступления, если оно не выдает такое лицо в связи с преступлением, к которому применяется настоящая статья, обязано, без каких бы то ни было исключений по просьбе Государства-участника, запрашивающего выдачу, передать дело без неоправданных задержек своим компетентным органам для цели преследования. Эти органы принимают свое решение и осуществляют производство таким же образом, как и в случае любого другого преступления опасного характера согласно внутреннему законодательству этого Государства-участника. Заинтересованные Государства-участники сотрудничают друг с другом, в частности по процессуальным вопросам и вопросам доказывания, для обеспечения эффективности такого преследования.

12. Во всех случаях, когда Государству-участнику согласно его внутреннему законодательству разрешается выдавать или иным образом передавать одного из своих граждан только при условии, что это лицо будет возвращено в это государство для отбытия наказания, назначенного в результате судебного разбирательства или производства, в связи с которыми запрашивалась выдача или передача этого лица, и это Государство-участник и Государство-участник, запрашивающее выдачу этого лица, согласились с таким порядком и другими условиями, которые они могут счесть надлежащими, такая условная выдача или передача являются достаточными для выполнения обязательства, установленного в пункте 10 настоящей статьи.

13. Любому лицу, по делу которого осуществляется производство в связи с любым преступлением, к которому применяется настоящая статья, гарантируется справедливое обращение на всех стадиях производства, включая осуществление всех прав и гарантий, предусмотренных Международным пактом о гражданских и политических правах и внутренним законодательством Государства-участника, на территории которого находится это лицо.

14. Ничто в настоящей Конвенции не толкуется как устанавливающее обязательство выдачи, если у запрашиваемого Государства-участника имеются существенные основания полагать, что просьба о выдаче имеет целью преследование или наказание какого-либо лица по причине его пола, расы, языка, вероисповедания, гражданства или этнического происхождения или что удовлетворение этой просьбы нанесло бы ущерб положению этого лица по любой из этих причин.

15. До отказа в выдаче запрашиваемое Государство-участник в надлежащих случаях проводит консультации с запрашивающим

Государством-участником, с тем чтобы предоставить ему достаточные возможности для изложения его мнений и представления информации, имеющей отношение к изложенным в его запросе фактам.

16. Государства-участники стремятся заключать двусторонние и многосторонние договоры или договоренности с целью осуществления или повышения эффективности выдачи.

17. Каждое Государство-участник назначает центральный орган, ответственный за получение запросов о выдаче и их выполнение. При сдаче на хранение Государством-участником его ратификационной грамоты или документа о принятии или утверждении настоящей Конвенции или присоединении к ней Генеральный секретарь Организации Объединенных Наций уведомляется о центральном органе, назначенном с этой целью.

Статья 48. Non bis in idem

1. Выдача не осуществляется, если компетентные органы запрашиваемого Государства-участника вынесли окончательное решение в отношении запрашиваемого к выдаче лица, в связи с преступлением которого запрашивается выдача. В выдаче может быть отказано, если компетентные органы запрашиваемого Государства-участника вынесли решение не осуществлять или прекратить судебное преследование в отношении того же преступления.

2. Выдача лица, по делу которого было вынесено окончательное судебное решение в третьем государстве, являющемся участником Конвенции, в связи с преступлением, в отношении которого запрашивается выдача, не производится:

a) если вышеупомянутое судебное решение освобождает его от ответственности;

b) если срок заключения или другая мера наказания, вынесенная в его отношении:

i) была полностью применена;

ii) стала полностью или в отношении не примененной части предметом помилования или амнистии;

c) если суд осудил преступника без наложения санкций.

3. Вместе с тем в случаях, упоминаемых в пункте 2, решение о выдаче может быть принято:

a) если преступление, в отношении которого было вынесено судебное решение, было совершено против лица, учреждения или любого субъекта, являющегося публичным должностным лицом запрашивающего государства;

b) если лицо, в отношении которого было вынесено судебное решение, является публичным должностным лицом запрашивающего государства;

c) если преступление, в отношении которого было вынесено судебное решение, было совершено полностью или частично на территории запрашивающего государства или в месте, рассматриваемом как его территория.

4. Положения пунктов 2 и 3 не препятствуют применению более широких внутренних норм, касающихся действия принципа non bis in idem, в отношении судебных решений по уголовным делам, вынесенных в другом государстве.

Статья 49. Взаимная правовая помощь

1. Государства-участники на взаимной основе оказывают друг другу правовую помощь в целях проведения расследований, преследования или судебного разбирательства в связи с преступлениями и иными противоправными деяниями, совершенными в сфере использования ИКТ.

2. Каждое Государство-участник принимает такие законодательные и иные меры, какие могут быть необходимы для выполнения обязательств, изложенных в статьях 55, 56, 59–62, 66 настоящей Конвенции. Каждое Государство-участник рассматривает также возможность увеличения (продления или приостановления) сроков давности в целях обеспечения неотвратимости ответственности.

3. За исключением случаев, когда положениями статей настоящей главы предусматривается иное, взаимная правовая помощь оказывается на условиях, предусмотренных внутренним законодательством запрашиваемого Государства-участника или положениями применимых договоров о взаимной правовой помощи, включая основания, на которых запрашиваемое Государство-участник может отказаться от сотрудничества полностью или частично.

4. Каждое Государство-участник назначает центральный орган, ответственный за получение запросов о взаимной правовой помощи и их выполнение. При сдаче на хранение Государством-участником его ратификационной грамоты или документа о принятии или утверждении настоящей Конвенции или присоединении к ней Генеральный секретарь Организации Объединенных Наций уведомляется о центральном органе, назначенном с этой целью.

Статья 50. Экстренная взаимная помощь

1. Для целей настоящей статьи чрезвычайная ситуация означает ситуацию, в которой существует значительный и неминуемый риск для жизни или безопасности любого физического лица.

2. Каждое Государство-участник может обратиться к другому Государству-участнику за взаимной помощью в кратчайшие сроки, если оно считает, что существует чрезвычайная ситуация. Запрос в соответствии с настоящей статьей должен включать, помимо прочего необходимого содержания, описание фактов, свидетельствующих о том, что существует чрезвычайная ситуация и связь с ней запрашиваемой помощи.

3. Запрашиваемое Государство-участник принимает такой запрос в электронной форме. Однако оно может потребовать обеспечить соответствующий уровень безопасности и аутентификации, прежде чем принимать запрос.

4. Запрашиваемое Государство-участник может в кратчайшие сроки запросить дополнительную информацию для оценки запроса. Запрашивающее Государство-участник предоставляет такую дополнительную информацию в возможно кратчайшие сроки.

5. Убедившись в наличии чрезвычайной ситуации и удовлетворении других требований, необходимых для оказания взаимной помощи, запрашиваемое Государство-участник отвечает на запрос в возможно кратчайшие сроки.

6. Каждое Государство-участник обеспечивает, чтобы должностное лицо его компетентного органа, отвечающее на запросы о взаимной помощи в соответствии со статьями 49 и 52 настоящей Конвенции, было доступно круглосуточно и без выходных для целей реагирования на запрос, направленный в соответствии с данной статьей.

7. Компетентные органы, отвечающие за взаимную помощь запрашивающего и запрашиваемого Государств-участников, могут договориться о том, чтобы результаты выполнения запроса в соответствии с настоящей статьей или их предварительная копия могли быть предоставлены запрашивающему Государству-участнику через альтернативный канал связи, отличный от обычно используемого для направления запроса об оказании правовой помощи.

8. В случае возникновения чрезвычайной ситуации запросы могут направляться непосредственно компетентными органами запрашивающего Государства-участника в соответствующие компетентные органы запрашиваемого Государства-участника или через каналы Интерпола или сети 24/7 в соответствии со статьей 66 настоящей Конвенции. В любых таких случаях копия запроса направляется одновременно в центральный орган запрашиваемого Государства-участника через центральный орган запрашивающего Государства-участника. Если запрос направляется непосредственно в центральный орган запрашиваемого Государства-участника и этот

орган не является компетентным органом по исполнению запроса, он передает запрос компетентному органу и сообщает центральному органу запрашивающего Государства-участника о передаче такого запроса. Каждое Государство-участник при подписании настоящей Конвенции или при сдаче на хранение ратификационной грамоты или документа о принятии, утверждении или присоединении может сообщить Генеральному секретарю Организации Объединенных Наций, что в целях эффективности запросы, поданные в соответствии с настоящим пунктом, должны направляться только в центральный орган.

Статья 51. Информация, предоставляемая в инициативном порядке

1. Государство-участник может с соблюдением норм своего внутреннего законодательства направить без предварительного запроса другого Государства-участника информацию, полученную в рамках своего расследования, когда, по его мнению, раскрытие такой информации могло бы помочь другому Государству-участнику начать или провести расследование, преследование или судебное разбирательство в отношении преступлений или иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией, или могло бы повлечь за собой направление этим Государством-участником запроса о сотрудничестве в соответствии с положениями настоящей главы.

2. Прежде чем предоставить такую информацию, предоставляющее Государство-участник может просить о соблюдении ее конфиденциальности или определенных условий для ее использования. Если получающее Государство-участник не может выполнить такую просьбу, оно уведомляет об этом предоставляющее Государство-участника, которое определяет затем, следует ли тем не менее предоставить такую информацию. Если получающее Государство-участник принимает информацию на указанных условиях, они носят для него обязательный характер.

Статья 52. Процедуры направления запросов о взаимной правовой помощи в отсутствие применимых международных договоров

1. В случае, когда между запрашивающим и запрашиваемым Государствами-участниками нет действующего договора о взаимной правовой помощи, применяются положения пунктов 2–8 настоящей статьи. При наличии такого договора положения настоящей статьи не применяются, если только заинтересованные Государства-участники не соглашаются применять взамен любые или все последующие положения настоящей статьи.

2. a) Каждое Государство-участник назначает центральный орган или органы, которые направляют запросы о взаимной правовой помощи и отвечают на них, организуют исполнение таких запросов или их передачу органам, в компетенцию которых входит их выполнение;

b) центральные органы или иные органы, указанные в подпункте «a», взаимодействуют друг с другом непосредственно;

c) каждое Государство-участник при сдаче на хранение своей ратификационной грамоты или своего документа о принятии, одобрении или присоединении сообщает Генеральному секретарю Организации Объединенных Наций наименования и адреса органов, назначенных в соответствии с настоящим пунктом;

d) Генеральный секретарь Организации Объединенных Наций составляет и постоянно обновляет реестр центральных органов, назначенных Государствами-участниками. Каждое Государство-участник обеспечивает, чтобы в этом реестре всегда содержались актуализированные сведения.

3. При исполнении запроса о взаимной правовой помощи органы запрашиваемого Государства-участника применяют законодательство своего государства. По просьбе запрашивающего органа могут применяться процессуальные нормы запрашивающего Государства-участника, если они не противоречат основным принципам правовой системы запрашиваемого Государства-участника.

4. Запрашиваемое Государство-участник может отказать в оказании правовой помощи, если:

a) запрос касается преступления, рассматриваемого запрашиваемым Государством-участником как преступление или как правонарушение, связанное с преступлением против государства;

b) по его мнению, выполнение запроса причинит ущерб его суверенитету безопасности, публичному порядку или иным существенным интересам.

5. Запрашиваемое государство-участник может отложить принятие мер по запросу, если такие меры препятствовали бы уголовным расследованиям или судебным разбирательствам, проводимым его компетентными органами.

6. Прежде чем отказать в предоставлении правовой помощи или отсрочить ее оказание, запрашиваемое Государство-участник по мере необходимости после консультаций с запрашивающим Государством-участником рассматривает возможность удовлетворения запроса частично или на таких условиях, какие оно сочтет необходимыми.

7. Запрашиваемое Государство-участник в кратчайшие сроки информирует запрашивающее Государство-участник о результатах выполнения запроса о правовой помощи. В случае отказа в выполнении запроса или отсрочки его выполнения сообщаются причины такого отказа или отсрочки.

8. Запрашивающее Государство-участник может просить запрашиваемое Государство-участника обеспечить конфиденциальность факта и предмета любого запроса, направленного в соответствии с положениями настоящей главы, но лишь в той степени, которая согласуется с его выполнением. Если запрашиваемое государство-участник не может выполнить просьбу о сохранении конфиденциальности, оно незамедлительно сообщает об этом запрашивающему Государству-участнику, которое затем принимает решение о том, следует ли, тем не менее, исполнять запрос.

Статья 53. Проведение допроса и иных процессуальных действий с использованием систем видеоконференции или телефонной конференции

1. Компетентные органы Государства-участника по взаимному согласию могут оказывать правовую помощь путем использования систем видеоконференции или телефонной конференции.

2. Использование систем видеоконференции или телефонной конференции осуществляется в соответствии с законодательством запрашиваемого Государства-участника. Если запрашиваемое Государство-участник не имеет доступа к техническим средствам для проведения видеоконференции, такие средства по взаимной договоренности могут быть предоставлены ему запрашивающим Государством-участником.

Статья 54. Полномочия дипломатических представительств и консульских учреждений

1. Государства-участники имеют право вручать документы собственным гражданам через свои дипломатические представительства или консульские учреждения.

2. Государства-участники имеют право по поручению своих компетентных органов допрашивать собственных граждан через свои дипломатические представительства или консульские учреждения, в том числе с использованием систем видео-конференц-связи или телефонной конференции.

3. В случаях, указанных в пунктах 1 и 2 настоящей статьи, нельзя применять средства принуждения или угрозу ими.

Статья 55. Конфиденциальность и ограничения на использование информации

1. В случае отсутствия между запрашивающим и запрашиваемым Государствами-участниками действующего договора о взаимной правовой помощи, опирающегося на единообразное или основанное на принципе взаимности законодательство, применяются положения настоящей статьи. Положения настоящей статьи при наличии такого договора или законодательства не применяются, если только заинтересованные Государства-участники не соглашаются применять вместо последних любые или все последующие положения настоящей статьи.

2. В ответ на просьбу запрашиваемое Государство-участник может выдвинуть следующие условия предоставления информации или материала:

a) сохранение их конфиденциальности, если без такого условия просьба о взаимной правовой помощи не могла бы быть выполнена;

b) неиспользование для других расследований или судебных разбирательств, которые не указываются в просьбе.

3. Если запрашивающее Государство-участник не может выполнить одно из условий, упомянутых в пункте 2 настоящей статьи, оно незамедлительно информирует об этом другое Государство-участника, которое затем решает, может ли быть предоставлена такая информация. Если запрашивающее Государство-участник соглашается выполнить эти условия, они приобретают для него обязательную силу.

4. Любое Государство-участник, предоставляющее информацию или материал на упомянутых в пункте 2 настоящей статьи условиях, может в связи с одним из условий потребовать от другого Государства-участника разъяснений относительно имевшего место использования такой информации или материала.

Статья 56. Защита персональных данных

1. Персональные данные, передаваемые одним Государством-участником другому Государству-участнику на основании запроса, сделанного в соответствии с настоящей Конвенцией, могут быть использованы Государством-участником, которому переданы эти данные, только для целей производства по уголовному, административному или гражданскому делу, других судебных или административных процедур, напрямую связанных с этим производством, а также для предотвращения непосредственной и серьезной угрозы общественной безопасности и безопасности лиц, чьи персональные данные передаются.

2. Такие персональные данные не могут быть переданы третьей стороне без предварительного письменного согласия Государства-участника, из которого были переданы данные, или субъекта персональных данных.

3. Государство-участник, которое передает персональные данные на основании запроса, сделанного в соответствии с настоящей Конвенцией, может потребовать от Государства-участника, которому переданы данные, предоставления информации об их использовании.

Статья 57. Передача уголовного производства

Государства-участники рассматривают возможность взаимной передачи производства в целях уголовного преследования в связи с преступлением, охватываемым настоящей Конвенцией, в случаях, когда считается, что такая передача отвечает интересам надлежащего отправления правосудия, в частности в случаях, когда затрагиваются несколько юрисдикций, для обеспечения объединения уголовных дел.

Статья 58. Передача осужденных лиц

Государства-участники рассматривают возможность заключения двусторонних или многосторонних договоров или иных договоренностей о передаче лиц, осужденных к тюремному заключению или другим видам лишения свободы за преступления, признанные таковыми в соответствии с настоящей Конвенцией, с тем чтобы такие лица могли отбывать срок наказания на территории этих Государств-участников.

Статья 59. Оперативное обеспечение сохранности информации в электронной форме

1. Любое Государство-участник может просить другое Государство-участника дать указание или принять иные меры с целью безотлагательно обеспечить сохранность информации, которая хранится или обрабатывается с использованием ИКТ на территории этого Государства-участника и в отношении которой запрашивающее Государство-участник намеревается в рамках взаимной правовой помощи направить запрос об обыске, выемке или об ином обеспечении сохранности или получении этой информации.

2. В запросе об обеспечении сохранности информации, направляемом в соответствии с пунктом 1 настоящей статьи, указываются:

a) наименование запрашивающего органа;

b) краткое изложение основных фактов, характер расследования, преследования или судебного разбирательства, к которым относится запрос;

c) информация в электронной форме, подлежащая сохранению, и ее связь с преступлением или правонарушением, по которому направлен запрос;

d) любые имеющиеся сведения, идентифицирующие владельца информации или местоположение устройства ИКТ;

e) обоснование необходимости обеспечения сохранности информации;

f) сообщение о том, что это Государство-участник намеревается в рамках взаимной правовой помощи направить запрос об обыске, выемке или об ином обеспечении сохранности этой информации.

3. По получении такого запроса от другого Государства-участника запрашиваемое Государство-участник в соответствии со своим внутренним законодательством принимает надлежащие меры для оперативного обеспечения сохранности информации, указанной в пункте 1 настоящей статьи. Запрашиваемое Государство-участник может исполнить частично либо полностью запрос об обеспечении сохранности информации, даже если деяние, послужившее основанием для запроса, не является уголовно наказуемым в запрашиваемом Государстве-участнике.

4. В исполнении запроса об обеспечении сохранности информации может быть отказано, если запрашиваемое Государство-участник полагает, что исполнение такого запроса может нанести ущерб его суверенитету, безопасности или другим существенным интересам.

5. Если запрашиваемое Государство-участник полагает, что исполнение запроса, указанного в пункте 1 настоящей статьи, не обеспечит в дальнейшем сохранности информации или поставит под угрозу обеспечение конфиденциальности, или иным образом помешает проводимому расследованию, преследованию или судебному разбирательству, оно незамедлительно уведомляет об этом запрашивающее Государство-участника. На основании такого уведомления запрашивающее Государство-участник принимает решение о необходимости исполнения запроса.

6. Любое обеспечение сохранности информации, предпринятое в рамках исполнения запроса, указанного в пункте 1 настоящей статьи, производится на срок не менее 90 дней для того, чтобы запрашивающее Государство-участник могло направить запрос об обыске, выемке или об ином обеспечении сохранности этой информации. После получения такого запроса запрашиваемое Государство-участник сохраняет эту информацию до принятия решения по запросу.

Статья 60. Оперативное предоставление сохраненных технических параметров трафика

1. Если в ходе исполнения запроса об обеспечении сохранности информации в соответствии со статьей 59 настоящей Конвенции запрашиваемому Государству-участнику станет известно, что в передаче информации участвовал поставщик услуг с территории иного государства, оно оперативно раскрывает в порядке, установленном национальным законодательством, запрашивающему Государству-участнику технические параметры трафика в объеме, позволяющем идентифицировать этого поставщика услуг и определить маршрут передачи информации, сохранение которой запрашивается.

2. В исполнении запроса об обеспечении сохранности информации может быть отказано, если запрашиваемое Государство-участник полагает, что исполнение такого запроса может нанести ущерб его суверенитету, безопасности или другим существенным интересам.

Статья 61. Взаимная помощь по сбору технических параметров трафика в режиме реального времени

1. Государство-участник по запросу другого Государства-участника осуществляет на своей территории или территории, находящейся под его юрисдикцией, сбор технических параметров трафика в режиме реального времени и затем, в соответствии с процедурами, предусмотренными внутренним законодательством, при наличии соответствующих оснований передает собранную информацию запрашивающему Государству-участнику.

2. В запросе, направляемом в соответствии с пунктом 1 настоящей статьи, указываются:

a) наименование запрашивающего органа;

b) краткое изложение основных фактов, характер расследования, преследования или судебного разбирательства, к которым относится запрос;

c) информация в электронной форме, относительно которой требуется сбор технических параметров трафика, и ее связь с преступлением или иным противоправным деянием;

d) любые имеющиеся сведения, идентифицирующие владельца/пользователя информации или местоположение устройства ИКТ;

e) обоснование необходимости сбора технических параметров трафика; обоснование указанного периода сбора технических параметров трафика;

f) период сбора технических параметров трафика.

Статья 62. Взаимная помощь по сбору информации в электронной форме

Государство-участник осуществляет на своей территории или территории, находящейся под его юрисдикцией, сбор информации в электронно-цифровой форме, включающей данные о содержании сообщений, в режиме реального времени, передаваемой с использованием ИКТ, в соответствии с процедурами, предусмотренными его внутренним законодательством. Предоставление другому Государству-участнику такой информации осуществляется в соответствии с внутренним законодательством Государства-участника, осуществляющего сбор информации, а также действующими договорами о взаимной правовой помощи.

Статья 63. Совместные расследования

По взаимному соглашению компетентные органы двух или более Государств-участников могут создавать совместные следственные группы для определенной цели и на ограниченный период, который может быть продлен по взаимному согласию, для проведения уголовных расследований в одном или нескольких Государствах-участниках, создавших группу. С этой целью Государства-участники рассматривают возможность заключения двусторонних или многосторонних соглашений или договоренностей. Состав группы определяется в соглашении.

Просьба о создании совместной следственной группы может исходить от любого заинтересованного Государства-участника. Группа создается в одном из государств-участников, в котором предполагается проведение расследования.

Государства-участники обеспечивают полное уважение суверенитета Государства-участника, на территории которого должно быть проведено такое расследование.

Статья 64. Специальные методы расследования

1. В целях эффективной борьбы с преступлениями в сфере использования ИКТ каждое Государство-участник в той мере, в какой это допускается основными принципами его внутреннего права, и на условиях, установленных законодательством, принимает в пределах своих возможностей необходимые меры, какие могут потребоваться, с тем чтобы разрешить надлежащее применение его компетентными органами контролируемых поставок и других специальных методов расследования, таких как электронное наблюдение или другие формы наблюдения, а также агентурные операции его компетентными органами на его территории и чтобы доказательства, собранные с помощью таких методов, допускались в суде.

2. Для цели расследования преступлений, охватываемых настоящей Конвенцией, Государства-участники поощряются к заключению при необходимости соответствующих двусторонних или многосторонних соглашений или договоренностей для использования таких специальных методов расследования в контексте сотрудничества на международном уровне. Такие соглашения или договоренности заключаются и осуществляются при полном соблюдении принципа суверенного равенства государств и реализуются в строгом соответствии с условиями этих соглашений или договоренностей.

3. В отсутствие соглашения или договоренности, указанных в пункте 2 настоящей статьи, решения об использовании таких специальных методов расследования на международном уровне принимаются в каждом отдельном случае и могут при необходимости учитывать финансовые договоренности и взаимопонимания в отношении осуществления юрисдикции заинтересованными Государствами-участниками.

Статья 65. Сотрудничество между правоохранительными органами

1. Государства-участники тесно сотрудничают друг с другом, действуя сообразно своим внутренним правовым и административным системам, в целях повышения эффективности правоприменительных мер для борьбы с преступлениями, охватываемыми настоящей Конвенцией. Государства-участники, в частности, принимают эффективные меры, направленные на:

a) укрепление или, где это необходимо, установление каналов связи между их компетентными органами, учреждениями и службами, с тем чтобы обеспечить надежный и быстрый обмен информацией обо всех аспектах преступлений, охватываемых настоящей Конвенцией, включая, если заинтересованные Государства-участники сочтут это надлежащим, связи с другими видами преступной деятельности;

b) сотрудничество с другими Государствами-участниками в проведении расследований в связи с преступлениями, охватываемыми настоящей Конвенцией, в целях выявления:

i) личности, местонахождения и деятельности лиц, подозреваемых в участии в совершении таких преступлений, или местонахождения других причастных лиц;

ii) перемещения доходов от преступлений или имущества, полученного в результате совершения таких преступлений;

iii) перемещения имущества, орудий, оборудования или других средств, использовавшихся или предназначавшихся для использования при совершении таких преступлений;

c) передачу: предметов, которые были использованы при совершении преступлений, в том числе орудий преступлений; предметов, которые были приобретены в результате преступлений или в качестве вознаграждения за них, или же предметов, которые преступник получил взамен предметов, приобретенных таким образом; и предметов, которые могут иметь значение доказательств в уголовном деле;

d) обмен в надлежащих случаях с другими Государствами-участниками информацией о конкретных средствах и методах, применяемых для совершения преступлений, охватываемых настоящей Конвенцией, включая образцы вредоносного программного обеспечения, использование поддельных удостоверений личности, фальшивых, измененных или поддельных документов и других средств для сокрытия противоправной деятельности;

e) содействие эффективной координации между их компетентными органами, учреждениями и службами и поощрение обмена сотрудниками и другими экспертами, включая, при условии заключения заинтересованными Государствами-участниками двусторонних соглашений или договоренностей, направление сотрудников по связям;

f) обмен представляющей интерес информацией и проведение скоординированных мероприятий с целью заблаговременного выявления преступлений, охватываемых настоящей Конвенцией.

2. Для целей практического применения настоящей Конвенции Государства-участники рассматривают возможность заключения двусторонних или многосторонних соглашений или договоренностей о непосредственном сотрудничестве между их правоохранительными органами, а в тех случаях, когда такие соглашения или договоренности уже имеются, — их совершенствования. В отсутствие таких соглашений или договоренностей между заинтересованными Государствами-участниками Государства-участники могут рассматривать настоящую Конвенцию в качестве основы для взаимного сотрудничества между правоохранительными органами в отношении преступлений, охватываемых настоящей Конвенцией. В надлежащих случаях Государства-участники в полной мере используют соглашения или договоренности, в том числе механизмы международных или региональных организаций, для расширения сотрудничества между своими правоохранительными органами.

Каждое Государство-участник может в экстренных ситуациях направлять запросы об оказании содействия или сообщения, связанные с такими запросами, используя оперативные средства связи, включая факсимильную связь или электронную почту, в той мере, в какой такие средства обеспечивают соответствующие уровни безопасности и подтверждение подлинности (включая, если необходимо, использование шифрования), с последующим официальным подтверждением, если того требует запрашиваемое Государство-участник. Запрашиваемое Государство-участник принимает такой запрос и отвечает на него с помощью любых аналогичных оперативных средств связи. Запрашиваемое Государство-участник может оставить за собой право направить ответ после получения оригинала запроса, о чем уведомляет депозитария.

Статья 66. Сеть 24/7

1. Каждое Государство-участник назначает контактный центр, работающий 24 часа в сутки 7 дней в неделю и призванный обеспечивать оперативное содействие в проведении расследований, преследований или судебных разбирательств в связи с преступлениями, имеющими отношение к компьютерным системам и данным, или в сборе доказательств в электронно-цифровой форме в отношении преступлений. Такая помощь включает поддержку применения или, если это допускается внутренним правом или практикой, непосредственное применение следующих мер:

a) оказание технической консультативной помощи;

b) обеспечение сохранности данных в целях сбора доказательств и последующего предоставления информации в соответствии с его внутренним законодательством, а также действующими договорами о взаимной правовой помощи.

2. Каждое Государство-участник принимает меры для предоставления квалифицированного персонала и оборудования с целью облегчения функционирования такой сети.

Раздел 2. МЕРЫ ПО ВОЗВРАЩЕНИЮ ИМУЩЕСТВА

Статья 67. Общее положение

Государства-участники самым широким образом сотрудничают друг с другом и предоставляют друг другу взаимную правовую помощь по возвращению имущества, полученного преступным путем, в соответствии с положениями настоящей Конвенции и внутренним законодательством и с учетом соответствующих инициатив международных региональных и межрегиональных организаций по противодействию отмыванию денежных средств.

Статья 68. Предупреждение и выявление переводов доходов от преступлений

1. Государство-участник принимает все необходимые меры, позволяющие в соответствии с внутренним законодательством получать от финансовых учреждений, а также организаций, осуществляющих деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, на которые распространяется его юрисдикция, информацию о личности клиентов и собственников-бенефициаров, в отношении которых имеется информация об их возможной причастности или о возможной причастности членов их семей или тесно связанных с ними партнеров или лиц, действующих от их имени, к совершению преступлений, предусмотренных положениями настоящей Конвенции, включая информацию о счетах всех вышеперечисленных лиц.

2. Государство-участник принимает все необходимые меры, позволяющие в соответствии с внутренним законодательством требовать от финансовых учреждений, а также организаций, осуществляющих деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, принятия разумных мер контроля в отношении счетов, которые пытаются открыть или которые ведут лица, указанные в пункте 1 настоящей статьи.

3. Меры, указанные в пунктах 1 и 2 настоящей статьи, в разумной степени призваны выявлять подозрительные операции для целей представления информации о них компетентным органам и не должны толковаться как препятствующие или запрещающие финансовым учреждениям, а также организациям, осуществляющим деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, вести дела с любым законным клиентом.

4. С целью содействия осуществлению мер, предусмотренных в пунктах 1 и 2 настоящей статьи, каждое Государство-участник в надлежащих случаях уведомляет финансовые учреждения, а также организации, осуществляющие деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, на которые распространяется его юрисдикция, по просьбе другого Государства-участника или по своей собственной инициативе, о личностях конкретных физических или юридических лиц, в отношении счетов которых от таких учреждений и организаций будет ожидаться применение более жестких мер контроля, в дополнение к тем лицам, личности которых финансовые учреждения, а также организации, осуществляющие деятельность, связанную с обо-

ротом цифровых финансовых активов и цифровой валюты, могут установить в ином порядке.

5. Каждое Государство-участник осуществляет меры для обеспечения того, чтобы его финансовые учреждения, а также организации, осуществляющие деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, сохраняли в течение надлежащего срока должную отчетность о счетах и операциях, к которым причастны лица, упомянутые в пункте 1 настоящей статьи, в которую должна включаться как минимум информация, касающаяся личности клиента, а также, насколько это возможно, собственника-бенефициара.

6. С целью предупреждения и выявления переводов доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, каждое Государство-участник осуществляет надлежащие и действенные меры для предупреждения при помощи своих регулирующих и надзорных органов учреждения банков, которые не имеют физического присутствия и которые не аффилированы с какой-либо регулируемой финансовой группой. Кроме того, Государства-участники рассматривают возможность установления по отношению к своим финансовым учреждениям, а также организациям, осуществляющим деятельность, связанную с оборотом цифровых финансовых активов и цифровой валюты, требований отказываться вступать в корреспондентские банковские отношения с такими учреждениями или продолжать такие отношения, а также остерегаться устанавливать отношения с иностранными финансовыми учреждениями, разрешающими использование счетов в них банками, которые не имеют физического присутствия или которые не аффилированы с какой-либо регулируемой финансовой группой.

7. Каждое Государство-участник рассматривает возможность создания в соответствии со своим внутренним законодательством эффективных систем, предусматривающих раскрытие финансовой информации относительно лиц, в отношении которых имеется информация о возможной причастности к совершению преступлений, предусмотренных положениями настоящей Конвенции, и устанавливает надлежащие санкции за несоблюдение требований, указанных в настоящей статье. Каждое Государство-участник рассматривает также возможность принятия таких мер, какие могут потребоваться, с тем чтобы позволить своим компетентным органам осуществлять обмен такой информацией с компетентными органами в других Государствах-участниках, когда это необходимо для расследования и принятия мер по возвращению доходов от пре-

ступлений, признанных таковыми в соответствии с настоящей Конвенцией.

Статья 69. Меры для непосредственного возвращения имущества

Каждое Государство-участник в соответствии со своим внутренним законодательством принимает такие законодательные или иные меры, которые могут потребоваться, с тем чтобы:

a) разрешить другому Государству-участнику, его гражданам и лицам без гражданства, постоянно проживающим на его территории, и юридическим лицам, учрежденным или имеющим постоянное представительство на его территории, предъявлять в суды этого Государства-участника гражданские иски об установлении имущественного права, нарушенного в результате совершения какого-либо из преступлений или иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией;

b) позволить своим судам выносить решения о выплате компенсации или возмещении ущерба, нанесенного в результате совершения таких преступлений и иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией; и

c) позволить своим судам или компетентным органам при вынесении решений о конфискации признавать полностью или частично требования другого Государства-участника, его граждан и лиц без гражданства, постоянно проживающих на его территории, и юридических лиц, учрежденных или имеющих постоянное представительство на его территории, как законного собственника имущества, приобретенного в результате совершения какого-либо из преступлений или иных противоправных деяний, признанных таковыми в соответствии с настоящей Конвенцией.

Статья 70. Механизмы изъятия имущества посредством международного сотрудничества в деле конфискации

1. Каждое Государство-участник в целях предоставления взаимной правовой помощи в отношении имущества, приобретенного в результате совершения какого-либо из преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или средств совершения таких преступлений в соответствии со своим внутренним законодательством:

a) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам приводить в исполнение постановления о конфискации, вынесенные судами другого Государства-участника;

b) в пределах своей юрисдикции принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным

органам конфисковать имущество иностранного происхождения по судебному решению в связи с легализацией доходов, полученных в результате совершения преступления, признанного таковым в соответствии с положениями настоящей Конвенции;

c) рассматривает вопрос о принятии таких мер, какие могут потребоваться, с тем чтобы создать возможность для конфискации такого имущества без вынесения приговора в рамках уголовного производства по делам, когда преступник не может быть подвергнут преследованию по причине смерти, укрывательства или отсутствия или в других соответствующих случаях.

2. Каждое Государство-участник в целях предоставления взаимной правовой помощи по просьбе другого Государства-участника, в соответствии со своим внутренним законодательством:

a) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам налагать арест на имущество согласно постановлению об аресте, которое вынесено судом или другим компетентным органом запрашивающего Государства-участника и в котором излагаются разумные основания, позволяющие запрашиваемому Государству-участнику полагать, что существуют достаточные мотивы для принятия таких мер и что в отношении этого имущества будет в конечном итоге вынесено постановление о конфискации для целей пункта 1 (a) настоящей статьи;

b) принимает такие меры, какие могут потребоваться, с тем чтобы позволить своим компетентным органам налагать арест на имущество по запросу, в котором излагаются разумные основания, позволяющие запрашиваемому Государству-участнику полагать, что существуют достаточные мотивы для принятия таких мер и что в отношении этого имущества будет в конечном итоге вынесено постановление о конфискации для целей пункта 1 (a) настоящей статьи;

c) рассматривает вопрос о принятии дополнительных мер, с тем чтобы позволить своим компетентным органам сохранять имущество для целей конфискации, например, на основании иностранного постановления об аресте или предъявления уголовного обвинения в связи с приобретением подобного имущества.

3. Предоставление правовой помощи в соответствии с пунктом 2 настоящей статьи осуществляется на основании соответствующего запроса, направляемого в письменной форме.

4. При возникновении сомнения в подлинности или содержании запроса может быть запрошено его дополнительное подтверждение.

5. Запрос должен содержать следующую информацию:

a) наименование компетентного органа, запрашивающего содействие, и запрашиваемого компетентного органа;

b) изложение существа дела;

c) указание цели и обоснование запроса;

d) описание содержания запрашиваемого содействия;

e) копию постановления об аресте, если имеется;

f) любую другую информацию, которая может быть полезна для надлежащего исполнения запроса.

6. Запрос, переданный или подтвержденный в письменной форме, подписывается уполномоченным должностным лицом запрашивающего компетентного органа и удостоверяется печатью этого органа.

Статья 71. Международное сотрудничество в целях конфискации

1. Государство-участник, получившее от другого Государства-участника, под юрисдикцию которого подпадает какое-либо преступление, признанное таковым в соответствии с настоящей Конвенцией, запрос о конфискации упомянутого в пункте 1 статьи 70 настоящей Конвенции имущества, полученного в результате совершения преступлений, предусмотренных настоящей Конвенцией, или средств совершения таких преступлений, находящихся на его территории, в той степени, в которой это разрешено его внутренним законодательством:

a) направляет этот запрос своим компетентным органам с целью получения решения о конфискации и в случае вынесения такого решения приводит его в исполнение или

b) направляет своим компетентным органам решение о конфискации, вынесенное судом на территории запрашивающего Государства-участника, с целью его исполнения в том объеме, который указан в просьбе, и в той мере, в какой оно относится к находящемуся на территории запрашиваемого Государства-участника имуществу, полученному в результате совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или к средствам совершения таких преступлений.

2. По получении просьбы, направленной другим Государством-участником, под юрисдикцию которого подпадает какое-либо преступление, признанное таковым в соответствии с настоящей Конвенцией, запрашиваемое Государство-участник принимает меры для выявления или ареста имущества, полученного в результате совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, или средств совершения таких преступлений, упомянутых в пункте 1 (b) настоящей статьи, с целью по-

следующей конфискации, решение о которой выносится либо запрашивающим Государством-участником, либо в соответствии с просьбой согласно пункту 1 настоящей статьи запрашиваемым Государством-участником.

3. Решения или меры, предусмотренные в пунктах 1 и 2 настоящей статьи, принимаются запрашиваемым Государством-участником в соответствии с положениями его внутреннего законодательства и любыми двусторонними или многосторонними соглашениями или договоренностями, которыми оно может быть связано в отношениях с запрашивающим Государством-участником.

4. Каждое Государство-участник представляет Генеральному секретарю Организации Объединенных Наций тексты своих законов и правил, обеспечивающих осуществление положений настоящей статьи, а также тексты любых последующих изменений к таким законам и правилам или их описание.

5. В исполнении запроса, направленного в соответствии с настоящей статьей, может быть отказано или же обеспечительные меры могут быть сняты, если запрашиваемое Государство-участник своевременно не получит постановления компетентного органа запрашивающего Государства-участника или документов, необходимых для принятия компетентным органом запрашиваемого Государства-участника такого решения.

6. До снятия любой обеспечительной меры, принятой в соответствии с настоящей статьей, запрашиваемое Государство-участник, когда это возможно, предоставляет запрашивающему Государству-участнику возможность представить обоснование (изложить свои мотивы в пользу) продолжения осуществления такой меры.

7. Положения настоящей статьи не толкуются таким образом, чтобы наносился ущерб правам добросовестных третьих сторон.

Статья 72. Специальное сотрудничество

Без ущерба для своего внутреннего законодательства каждое Государство-участник стремится принимать меры, позволяющие ему в инициативном порядке и если это не наносит ущерб проводимым его компетентными органами уголовным расследованиям или судебным разбирательствам, направлять информацию об имуществе, полученном в результате совершения преступлений, признанных таковыми в соответствии с настоящей Конвенцией, другому Государству-участнику, когда оно считает, что раскрытие такой информации может послужить основанием для проведения уголовного расследования или судебного разбирательства компетентными органами получающего Государства-участника или может привести

к направлению этим Государством-участником запроса в соответствии с настоящей главой.

Статья 73. Возвращение похищенного имущества и распоряжение им

1. Государство-участник, конфисковавшее имущество в соответствии с положениями настоящей главы, распоряжается им, включая возвращение такого имущества его предыдущим законным собственникам согласно пункту 3 настоящей статьи и своему внутреннему законодательству.

2. Каждое Государство-участник принимает такие законодательные и иные меры, которые могут потребоваться для того, чтобы позволить своим компетентным органам возвращать конфискованное имущество, когда они действуют по запросу, направленному другим Государством-участником в соответствии с настоящей Конвенцией, с учетом прав добросовестных третьих сторон и в соответствии со своим внутренним законодательством.

3. В соответствии со статьей 71 настоящей Конвенции и пунктами 1 и 2 настоящей статьи запрашиваемое Государство-участник:

a) в случае хищения публичного имущества, если конфискация была произведена в соответствии со статьей 68 настоящей Конвенции и на основании окончательного судебного решения, вынесенного в запрашивающем Государстве-участнике, причем это требование может быть снято запрашиваемым Государством-участником, — возвращает конфискованное имущество запрашивающему Государству-участнику;

b) во всех других случаях в первоочередном порядке рассматривает вопрос о возвращении конфискованного имущества его предыдущим законным собственникам или выплате компенсации или возмещении ущерба потерпевшим от преступления.

4. В надлежащих случаях, если только Государства-участники не примут иного решения, запрашиваемое Государство-участник может вычесть разумные расходы, понесенные в ходе расследования или судебного разбирательства, которые привели к возвращению конфискованного имущества или распоряжению им согласно настоящей статье.

5. В целях достижения взаимоприемлемых договоренностей относительно окончательного распоряжения конфискованным имуществом Государства-участники могут проводить консультации и заключать отдельные соглашения.

Статья 74. Расходы

Обычные расходы, связанные с выполнением запроса, покрываются запрашиваемым Государством-участником, если заинтере-

сованные Государства-участники не договорились об ином. Если выполнение запроса требует существенных или чрезвычайных расходов, то Государства-участники проводят консультации с целью определения условий, на которых будет выполнен запрос, а также порядка покрытия расходов.

ГЛАВА V.ТЕХНИЧЕСКАЯ ПОМОЩЬ И ПОДГОТОВКА КАДРОВ

Статья 75.Общие принципы технической помощи

1. Государства-участники с учетом своих возможностей рассматривают вопрос о предоставлении друг другу широкой технической помощи, особенно в интересах развивающихся стран, в связи с их соответствующими планами и программами по борьбе с преступлениями в сфере ИКТ, включая подготовку кадров в областях, указанных в статье 76 настоящей Конвенции, а также подготовку кадров и оказание помощи и взаимный обмен соответствующим опытом и специальными знаниями, что будет способствовать международному сотрудничеству между Государствами-участниками по вопросам выдачи, взаимной правовой помощи.

2. Государства-участники активизируют, насколько это необходимо и возможно, усилия, направленные на максимальное повышение эффективности практических и учебных мероприятий в международных и региональных организациях и в рамках соответствующих двусторонних и многосторонних соглашений или договоренностей.

3. Государства-участники рассматривают возможность оказания друг другу содействия, по просьбе, в проведении оценок, исследований и разработок, касающихся видов, причин и последствий преступлений, совершаемых в сфере ИКТ в своих соответствующих странах, с целью разработки с участием компетентных органов, общества и частного сектора стратегий и планов действий по борьбе с этими видами преступлений.

4. Государства-участники поручают Управлению Организации Объединенных Наций по наркотикам и преступности оказывать Государствам-участникам профильную техническую помощь в целях содействия реализации программ и проектов по борьбе с преступлениями и иными правонарушениями в сфере ИКТ.

Статья 76. Подготовка кадров

1. Каждое Государство-участник, насколько это необходимо, разрабатывает, осуществляет или совершенствует конкретные программы подготовки своего персонала, несущего ответственность за предупреждение преступлений в сфере ИКТ и борьбу с ними.

Такие программы подготовки кадров могут затрагивать, среди прочего, следующие области:

a) эффективные меры по предупреждению, выявлению и расследованию преступлений в сфере ИКТ, а также наказанию за их совершение и борьбе с ними, включая методы сбора и использования доказательств в электронной форме и расследования;

b) наращивание потенциала в области разработки и планирования стратегической политики противодействия преступлениям в сфере ИКТ;

c) подготовка сотрудников компетентных органов по вопросам составления запросов о выдаче, взаимной правовой помощи и правоохранительном содействии, удовлетворяющих требованиям настоящей Конвенции;

d) предупреждение перевода доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, а также изъятие таких доходов;

e) выявление и приостановление операций по переводу доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

f) отслеживание перемещения доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией, и методов, используемых для перевода, сокрытия или утаивания таких доходов;

g) надлежащие и действенные правовые и административные механизмы и методы, способствующие изъятию и конфискации доходов от преступлений, признанных таковыми в соответствии с настоящей Конвенцией;

h) методы, используемые в защите потерпевших и свидетелей, которые сотрудничают с судебными и правоохранительными органами; и

i) подготовка сотрудников по вопросам, касающимся внутригосударственных и международных правил, и языковая подготовка.

2. Государства-участники при содействии Управления Организации Объединенных Наций по наркотикам и преступности и других международных организаций могут оказывать Государствам-участникам профильную помощь в подготовке кадров в целях содействия реализации национальных программ и проектов по борьбе с преступлениями в сфере ИКТ.

Статья 77. Обмен информацией

1. Каждое Государство-участник рассматривает возможность проведения, в консультации с экспертами, анализа тенденций пре-

ступности в сфере ИКТ на своей территории и обстоятельств совершения таких преступлений.

2. Государства-участники в целях разработки, насколько это возможно, общих определений, стандартов и методологий рассматривают возможность распространения статистических данных и аналитических знаний о преступлениях в сфере ИКТ, в том числе об оптимальных видах практики в деле предупреждения таких преступлений и борьбы с ними, и обмениваются этими данными между собой и через посредство международных и региональных организаций.

3. Каждое Государство-участник рассматривает возможность осуществления надлежащего контроля за своей политикой и практическими мерами по борьбе с преступлениями в сфере ИКТ, а также проведения оценки их эффективности.

ГЛАВА VI. МЕХАНИЗМЫ ВЫПОЛНЕНИЯ КОНВЕНЦИИ

Статья 78. Конференция Государств — участников Конвенции

1. Настоящим учреждается Конференция Государств — участников Конвенции в целях расширения возможностей Государств-участников и сотрудничества между ними для достижения целей, установленных в настоящей Конвенции, а также содействия выполнению настоящей Конвенции и проведения обзора хода ее осуществления.

2. Генеральный секретарь Организации Объединенных Наций созывает Конференцию Государств-участников не позднее чем через один год после вступления в силу настоящей Конвенции. Впоследствии в соответствии с правилами процедуры, принятыми Конференцией Государств-участников, проводятся очередные сессии Конференции.

3. Конференция Государств-участников принимает правила-процедуры и правила, регулирующие осуществление видов деятельности, указанных в настоящей статье, в том числе правила, касающиеся допуска и участия наблюдателей и оплаты расходов, понесенных при осуществлении этих видов деятельности.

4. Конференция Государств-участников согласовывает виды деятельности, процедуры и методы работы для достижения целей, изложенных в пункте 1 настоящей статьи, включая:

a) содействие деятельности Государств-участников согласно статьям 76–77 и главам II–VI настоящей Конвенции, в том числе путем поощрения мобилизации добровольных взносов;

b) содействие обмену между Государствами-участниками информацией о формах преступлений в сфере ИКТ и тенденциях

в этой области, а также об успешных методах предупреждения указанных преступлений, борьбы с ними, за исключением сведений, составляющих государственную тайну в соответствии с законодательством Государства-участника, и возвращения доходов от преступлений;

c) сотрудничество с соответствующими международными и региональными организациями и механизмами и международными неправительственными организациями;

d) надлежащее использование соответствующей информации, подготовленной другими международными и региональными механизмами в целях предупреждения преступлений в сфере ИКТ и борьбы с ними, во избежание излишнего дублирования работы;

e) периодическое рассмотрение вопроса об осуществлении настоящей Конвенции ее государствами-участниками; вынесение рекомендаций, касающихся совершенствования настоящей Конвенции и ее выполнения;

f) учет потребностей Государств-участников в технической помощи в связи с выполнением настоящей Конвенции и вынесение рекомендаций в отношении любых действий, которые она может считать необходимыми в связи с этим.

5. Для цели пункта 4 настоящей статьи Конференция Государств-участников получает необходимые сведения о мерах, принятых Государствами-участниками в ходе выполнения настоящей Конвенции, и трудностях, с которыми они при этом столкнулись, на основе предоставленной ими информации и через посредство таких дополнительных механизмов проведения обзора, какие могут быть созданы Конференцией Государств-участников.

6. Каждое Государство-участник представляет Конференции Государств-участников информацию о законодательных, административных и иных мерах, а также о своих программах, планах и практике, направленных на выполнение настоящей Конвенции, как это требуется Конференции Государств-участников. Конференция Государств-участников изучает вопрос о наиболее эффективных путях получения такой информации и принятия на ее основе соответствующих решений, включая, среди прочего, информацию, полученную от Государств-участников и от компетентных международных организаций. Могут быть рассмотрены также материалы, полученные от соответствующих международных неправительственных организаций, надлежащим образом аккредитованных в соответствии с процедурами, которые будут определены решением Конференции Государств-участников.

7. Согласно пунктам 4–6 настоящей статьи Конференция Государств-участников, если она сочтет это необходимым, учреждает любой соответствующий механизм или орган для содействия эффективному выполнению Конвенции.

Статья 79. Международная техническая комиссия

1. Конференция Государств-участников, в целях оказания содействия государствам в обзоре осуществления Конвенции, создает и учреждает Международную техническую комиссию по противодействию преступности в сфере ИКТ (МТК).

2. МТК является постоянно действующим органом, состоящим из 23 членов, и формируется по смешанному принципу: две трети ее членов представляются Конференцией Государств-участников, а одна треть — руководящими органами Международного союза электросвязи (МСЭ).

3. Члены Комиссии являются экспертами, обладающими непосредственным и значительным опытом в вопросах, касающихся дипломатии, международного и уголовного права, коммуникационных технологий или проведения соответствующих исследовательских разработок.

4. Члены Комиссии работают в течение пяти лет и могут назначаться повторно.

5. Сессии МТК созываются не реже одного раза в год в штаб-квартире МСЭ или Управления ООН по наркотикам и преступности или в таких местах и в такое время, которые могут быть указаны или утверждены Конференцией Государств-участников.

6. Комиссия разрабатывает правила-процедуры своей работы, подлежащие утверждению Конференцией Государств — участников Конвенции.

7. Комиссия проводит оценку технического прогресса в области ИКТ.

8. МТК через Конференцию Государств-участников докладывает о результатах своей работы Государствам-участникам и заинтересованным международным организациям.

Статья 80. Секретариат

1. Генеральный секретарь Организации Объединенных Наций обеспечивает необходимое секретариатское обслуживание Конференции Государств — участников Конвенции.

2. Секретариат:

а) организует сессии Конференции Государств-участников и МТК и обеспечивает их необходимым обслуживанием;

b) оказывает Государствам-участникам по их просьбе помощь в представлении информации Конференции Государств-участников и МТК и

c) обеспечивает необходимую координацию с секретариатами других соответствующих международных и региональных организаций и механизмов.

ГЛАВА VII. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Статья 81. Выполнение Конвенции

1. Каждое Государство-участник принимает в соответствии с основополагающими принципами своего внутреннего права необходимые меры, включая законодательные и административные меры, для обеспечения выполнения своих обязательств согласно настоящей Конвенции.

2. Каждое Государство-участник может принимать более строгие меры, чем меры, предусмотренные настоящей Конвенцией, для предупреждения преступлений в сфере ИКТ и борьбы с ними.

Статья 82. Урегулирование споров

В случае возникновения спора между Государствами-участниками относительно толкования или применения настоящей Конвенции они стремятся урегулировать его посредством переговоров, согласительной процедуры или арбитража либо иными мирными средствами, согласованными сторонами спора.

Статья 83. Подписание, ратификация, принятие и утверждение

1. Настоящая Конвенция открыта для подписания всеми государствами — членами ООН.

2. Настоящая Конвенция также открыта для подписания региональными организациями экономической интеграции при условии, что по меньшей мере одно из государств — членов такой организации подписало настоящую Конвенцию в соответствии с пунктом 1 настоящей статьи.

3. Настоящая Конвенция подлежит ратификации, принятию или утверждению. Документы о ратификации, принятии, утверждении или официальном одобрении сдаются на хранение Генеральному секретарю Организации Объединенных Наций. Региональная организация экономической интеграции может сдать на хранение свой документ о ратификации, принятии, утверждении или официальном одобрении, если по меньшей мере одно из ее государств-членов поступило таким же образом. В этом документе о ратификации, принятии, утверждении или официальном одобрении такая организация заявляет о сфере своей компетенции в отношении вопросов, регулируемых настоящей Конвенцией. Такая организация

также сообщает депозитарию о любом соответствующем изменении сферы своей компетенции.

Статья 84. Вступление в силу

1. Настоящая Конвенция вступает в силу на девяностый день после даты сдачи на хранение тридцатого документа о ратификации, принятии, утверждении или официальном одобрении. Для целей настоящего пункта любой такой документ, сданный на хранение региональной организацией экономической интеграции, не рассматривается в качестве дополнительных к документам, сданным на хранение государствами — членами такой организации.

2. Для каждого из государств или каждой из региональных организаций экономической интеграции, которые ратифицируют, принимают или утверждают настоящую Конвенцию после сдачи на хранение тридцатого документа о таком действии, настоящая Конвенция вступает в силу на тридцатый день после даты сдачи на хранение таким государством или организацией соответствующего документа или в дату вступления настоящей Конвенции в силу в соответствии с пунктом 1 настоящей статьи в зависимости от того, что наступает позднее.

Статья 85. Поправки

1. По истечении трех лет после вступления в силу настоящей Конвенции Государство-участник может предложить поправку и направить ее Генеральному секретарю Организации Объединенных Наций, который затем препровождает предлагаемую поправку Государствам-участникам и Конференции Государств — участников Конвенции в целях рассмотрения этого предложения и принятия решения по нему. Конференция Государств-участников прилагает все усилия для достижения консенсуса в отношении каждой поправки. Если все усилия по достижению консенсуса были исчерпаны и согласие не было достигнуто, то в качестве крайней меры для принятия поправки требуется большинство в две трети голосов Государств-участников.

2. В вопросах, входящих в сферу их компетенции, региональные организации экономической интеграции осуществляют свое право голоса согласно настоящей статье, располагая числом голосов, равным числу их государств-членов. Такие организации не осуществляют свое право голоса, если их государства-члены осуществляют свое право голоса, и наоборот.

3. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, подлежит ратификации, принятию или утверждению Государствами-участниками и соответствующими региональными организациями экономической интеграции.

4. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, вступает в силу в отношении Государства-участника или региональной организации экономической интеграции через 90 дней после даты сдачи на хранение Генеральному секретарю Организации Объединенных Наций ратификационной грамоты или документа о принятии или утверждении такой поправки двумя третями голосов.

5. Когда поправка вступает в силу, она становится обязательной для тех Государств-участников или региональных организаций экономической интеграции, которые выразили согласие быть связанными ею. Другие Государства-участники продолжают быть связанными положениями настоящей Конвенции или любыми поправками, ратифицированными, принятыми или утвержденными ими ранее.

Статья 86. Оговорки

Каждое Государство-участник путем письменного уведомления на имя Генерального секретаря Организации Объединенных Наций при подписании или сдаче на хранение ратификационной грамоты или документа о принятии, одобрении или присоединении может заявить, что оно воспользуется правом сделать оговорку относительно применения настоящей Конвенции. Оговорки к статьям 15–17, 19–20, 22–26, пункту 11 статьи 47 не допускаются.

Статья 87. Пересмотр Приложения

1. Любое Государство-участник может предлагать поправки к перечню международно-правовых документов, содержащемуся в Приложении к настоящей Конвенции.

2. Секретариат проводит мониторинг вновь принимаемых международно-правовых документов, которые могут затрагивать сферу применения настоящей Конвенции, и выносить предложения о внесении изменений в Приложение на рассмотрение очередной сессии Конференции Государств-участников.

3. Предложения о внесении поправок должны касаться только вступивших в силу универсальных и региональных международно-правовых документов, касающихся непосредственно международной преступности.

4. Проекты поправок, предложенных в соответствии с пунктом 1 настоящей статьи, направляются Генеральным секретарем Государствам-участникам. Если одна треть от общего числа Государств-участников, ратифицировавших настоящую Конвенцию, или более уведомляет Генерального секретаря ООН в течение шести месяцев со дня направления проекта поправки о своих возражениях против вступления поправки в силу, такая поправка не вступает в силу.

5. В вопросах, входящих в сферу их компетенции, региональные организации экономической интеграции осуществляют свое право голоса согласно настоящей статье, располагая числом голосов, равным числу их государств-членов. Такие организации не осуществляют свое право голоса, если их государства-члены осуществляют свое право голоса, и наоборот.

6. Если менее одной трети от общего числа Государств-участников, ратифицировавших настоящую Конвенцию, направляет свои возражения против вступления поправки в силу в адрес Генерального секретаря ООН в течение шести месяцев со дня направления проекта поправки, такая поправка вступает в силу в отношении Государств-участников, не возражающих против нее, через тридцать дней по истечении шести месяцев, предназначенных для внесения возражений.

7. На Конференции Государств-участников поправка принимается большинством голосов в две трети от общего числа Государств-участников, ратифицировавших настоящую Конвенцию. Такая поправка вступает в силу для Государств-участников, выразивших свое согласие на применение данной поправки, через тридцать дней со дня, следующего за днем принятия решения о принятии поправки.

8. Государство-участник, ранее возразившее против поправки, может изменить свое решение и уведомить депозитария о ее принятии. В таком случае данная поправка вступает в силу в отношении соответствующего Государства-участника через тридцать дней со дня, следующего за днем, когда оно уведомило Генерального секретаря ООН о ее принятии.

Статья 88. Денонсация

1. Государство-участник может денонсировать настоящую Конвенцию путем направления письменного уведомления Генеральному секретарю Организации Объединенных Наций. Такая денонсация вступает в силу по истечении шести месяцев после даты получения уведомления Генеральным секретарем.

2. Региональная организация экономической интеграции перестает быть участником настоящей Конвенции, когда все государства — члены этой организации денонсировали настоящую Конвенцию.

Статья 89. Депозитарий и языки

1. Депозитарием настоящей Конвенции назначается Генеральный секретарь Организации Объединенных Наций.

2. Подлинник настоящей Конвенции, английский, арабский, испанский, китайский, русский и французский тексты которой явля-

ются равно аутентичными, сдается на хранение Генеральному секретарю Организации Объединенных Наций.

В УДОСТОВЕРЕНИЕ ЧЕГО нижеподписавшиеся полномочные представители, должным образом уполномоченные на то своими правительствами, подписали настоящую Конвенцию.

ПРИЛОЖЕНИЕ

1. Единая конвенция о наркотических средствах (Нью-Йорк, 30 марта 1961 г.).

2. Конвенция о преступлениях и некоторых других актах, совершаемых на борту воздушных судов (Токио, 14 сентября 1963 г.).

3. Конвенция о борьбе с незаконным захватом воздушных судов (Гаага, 16 декабря 1970 г.).

4. Конвенция о психотропных веществах (Вена, 21 февраля 1971 г.).

5. Конвенция о предотвращении и наказании преступлений против лиц, пользующихся международной защитой, в том числе дипломатических агентов (Нью-Йорк, 14 декабря 1973 года).

6. Международная конвенция о борьбе с захватом заложников (Нью-Йорк, 17 декабря 1979 г.).

7. Конвенция о физической защите ядерного материала (Вена, 3 марта 1980 г.).

8. Конвенция о борьбе с незаконными актами, направленными против безопасности морского судоходства (Рим, 10 марта 1988 г.).

9. Конвенция Организации Объединенных Наций о борьбе против незаконного оборота наркотических средств и психотропных веществ (Вена, 19 декабря 1988 г.).

10. Международная конвенция о борьбе с бомбовым терроризмом (Нью-Йорк, 15 декабря 1997 г.).

11. Международная конвенция о борьбе с финансированием терроризма (Нью-Йорк, 9 декабря 1999 г.).

12. Международная конвенция о борьбе с актами ядерного терроризма (Нью-Йорк, 13 апреля 2005 г.).

Сведения об авторах

Агеев Владимир Владимирович, кандидат юридических наук, начальник ФКУ ГИАЦ МВД России

Бабушкин Александр Александрович, кандидат юридических наук, начальник отдела НИЦ-2 ФГКУ ВНИИ МВД России

Бегунов Александр Юрьевич, начальник высших академических курсов Академии управления МВД России

Воронцов Андрей Вячеславович, кандидат юридических наук, доцент, профессор кафедры организации оперативно-розыскной деятельности Академии управления МВД России

Городов Пётр Петрович, заместитель Генерального прокурора Российской Федерации

Давыдов Сергей Иванович, доктор юридических наук, заведующий кафедрой уголовного процесса и криминалистики Алтайского государственного университета

Жданов Юрий Николаевич, заслуженный юрист Российской Федерации, доктор юридических наук, профессор, президент Всероссийской полицейской ассоциации МПА

Завьялов Иван Александрович, кандидат юридических наук, доцент, заместитель начальника кафедры оперативно-розыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя

Искалиев Равиль Гарифуллаевич, кандидат юридических наук, доцент кафедры организации оперативно-розыскной деятельности Академии управления МВД России

Коваленко Вера Ивановна, доктор юридических наук, доцент, ведущий научный сотрудник сектора уголовного права, уголовного процесса и криминологии Института государства и права Российской академии наук

Кочубей Марианна Анатольевна, доктор юридических наук, председатель Научно-консультативного совета при Антитеррористическом центре государств — участников СНГ

Кузнецов Станислав Константинович, кандидат юридических наук, заместитель председателя правления Сбербанка России

Кузьмин Николай Александрович, кандидат юридических наук, доцент, начальник кафедры оперативно-розыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя

Лапунова Юлия Андреевна, кандидат юридических наук, доцент, заместитель начальника кафедры организации оперативно-розыскной деятельности Академии управления МВД России

Ларина Елена Сергеевна, ведущий аналитик Института системно-стратегического анализа

Маслов Алексей Александрович, доктор юридических наук, главный научный сотрудник НИЦ-2 ФГКУ ВНИИ МВД России

Морозов Андрей Владимирович, кандидат юридических наук, заместитель начальника 5-го Управления ГУНК МВД России

Наливайко Евгений Олегович, преподаватель кафедры оперативно-розыскной деятельности органов внутренних дел Дальневосточного юридического института МВД России

Овчинский Анатолий Семёнович, доктор технических наук, профессор, академик Российской академии естественных наук, профессор кафедры информационной безопасности учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя

Овчинский Владимир Семёнович, заслуженный юрист Российской Федерации, доктор юридических наук, советник министра внутренних дел Российской Федерации

Осипенко Анатолий Леонидович, доктор юридических наук, профессор, заместитель начальника Краснодарского университета МВД России по научной работе

Парфёнов Александр Вадимович, кандидат юридических наук, доцент, начальник кафедры организации оперативно-розыскной деятельности Академии управления МВД России

Саркисян Гор Георгиевич, кандидат юридических наук, старший преподаватель кафедры организации оперативно-розыскной деятельности Академии управления МВД России

Смирнов Александр Александрович, кандидат юридических наук, ответственный секретарь Научно-консультативного совета при Антитеррористическом центре государств — участников СНГ

Сундиев Игорь Юрьевич, доктор философских наук, профессор, главный научный сотрудник НИЦ-2 ФГКУ ВНИИ МВД России, вице-президент Всероссийской криминологической ассоциации

Телков Александр Валериевич, кандидат юридических наук, доцент кафедры организации оперативно-розыскной деятельности Академии управления МВД России

Хромов Игорь Львович, доктор юридических наук, профессор, профессор кафедры оперативно-розыскной деятельности и специальной техники Московского университета МВД России имени В.Я. Кикотя

Эзрохин Павел Владимирович, кандидат юридических наук, заместитель начальника УУР ГУВД МВД России по Московской области

Яковец Евгений Николаевич, заслуженный юрист Российской Федерации, доктор юридических наук, профессор, ведущий научный сотрудник Центра исследования проблем российского права «Эквитас»

Список сокращений

ВНИИ — Всероссийский научно-исследовательский институт МВД России

ГИАЦ — Главный информационно-аналитический центр МВД России

ГУНК — Главное управление по контролю за оборотом наркотиков МВД России

ИИ — искусственный интеллект

ИКТ — информационно-коммуникационные технологии

ИТТ — информационные технологии и телекоммуникации

ОВД — органы внутренних дел

ОРД — оперативно-розыскная деятельность

ОРМ — оперативно-розыскные мероприятия

ФЗ об ОРД — Федеральный закон «Об оперативно-розыскной деятельности»

ЭВМ — электронно-вычислительная машина

Всероссийская полицейская ассоциация МПА

Общероссийская общественная организация «Всероссийская полицейская ассоциация МПА» (ВПА МПА) является Российской секцией МПА.

Международная полицейская ассоциация (МПА) создана в 1950 г. в Великобритании и в настоящее время в ее составе действуют 69 национальных секций, включая российскую.

Ассоциация является международной неправительственной организацией с консультативным (специальным) статусом при Экономическом и Социальном Совете ООН; с консультативным статусом при Организации американских государств (ОАГ) и ЮНЕСКО, также сотрудничает с Интерполом и Европолом.

ВПА МПА стала членом Международной полицейской ассоциации в июне 1994 г.

По состоянию на 1 сентября 2021 г. ВПА МПА объединяет региональные отделения из 72 субъектов Российской Федерации. В состав организации входят действующие сотрудники полиции, Росгвардии, Генеральной прокуратуры Российской Федерации, Следственного комитета Российской Федерации, Министерства Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий, Министерства обороны Российской Федерации, таможенных органов, Росфинмониторинга, а также ветераны указанных органов, вышедшие в отставку.

В состав Наблюдательного совета Ассоциации входят многие видные политические и общественные деятели Российской Федерации, в том числе Сопредседатель Ассоциации юристов России С.В. Степашин (Председатель Наблюдательного совета), Председатель Следственного комитета Российской Федерации генерал юстиции РФ А.И. Бастрыкин, Заместитель Генерального прокурора РФ П.П. Городов, Член Совета Федерации Федерального Собрания РФ Г.А. Рапота, Президент Российской автомобильной федерации В.Н. Кирьянов, Руководитель Федерального агентства по делам Содружества Независимых Государств Е.А. Примаков, Генеральный директор ФГУП «Космическая связь» А.К. Волин, Президент Московской школы управления «Сколково» А.В. Ша-

ронов, Председатель Российского совета ветеранов ОВД и ВВ генерал-полковник И.Ф. Шилов.

Экспертный совет возглавляет Президент Клуба Военачальников Российской Федерации, доктор экономических наук, генерал армии А.С. Куликов, а также в него входят заместитель министра МЧС России генерал-полковник В.Н. Яцуценко, Заместитель председателя Следственного комитета РФ генерал-майор юстиции С.Н. Горяйнов, Президент Торгово-промышленной палаты Республики Татарстан Ш.Р. Агеев, Президент Московской торгово-промышленной палаты В.М. Платонов, Торговый представитель РФ в Республике Индия А.Л. Рыбас и другие видные деятели.

Основными целями Международной полицейской ассоциации, как и всех входящих в нее национальных секций, включая российскую, являются развитие международного полицейского сотрудничества, повышение имиджа полицейских и доверия к ним со стороны граждан, обобщение и распространение передового опыта работы полицейских разных стран, обмен делегациями, проведение спортивных соревнований, поддержка и развитие полицейского туризма, а также социальная поддержка ветеранов правоохранительных органов и членов их семей.

В Москве ежегодно в январе проходит заседание Международного полицейского клуба, созданного по инициативе ВПА МПА, в работе которого принимают участие полицейские и военные атташе из разных стран, служащие при посольствах в Москве, представители Бюро по координации борьбы с организованной преступностью стран СНГ, президенты национальных секций МПА, руководители региональных отделений ВПА МПА.

В рамках заседания Клуба проходят конференции на различные темы, такие как «Полиция будущего», «Безопасность дорожного движения. Международный опыт», «Кибербезопасность и новые виды преступлений» и др. В ходе данных мероприятий вырабатываются рекомендации для изменения российского законодательства и учета международного опыта в деятельности правоохранительных органов России.

Ассоциация активно участвует в развитии спорта, и под ее эгидой проходят спортивные соревнования сотрудников правоохранительных органов как в Российской Федерации, так и за рубежом (хоккей, футбол, дзюдо, стрельба и т.д.).

Кроме того, при участии и поддержке Ассоциации осуществляется проведение кинофестивалей (Международный фестиваль детективных фильмов «DetectiveFEST»), творческих вечеров и других мероприятий культурного обмена.

Ежегодно проводится Всемирный конгресс МПА с участием всех стран — членов организации.

ФЗ № 436-ФЗ	Издание не подлежит маркировке в соответствии с п. 1 ч. 2 ст. 1

Научное издание

ОПЕРАТИВНО-РОЗЫСКНАЯ ДЕЯТЕЛЬНОСТЬ В ЦИФРОВОМ МИРЕ

СБОРНИК НАУЧНЫХ ТРУДОВ

Под редакцией *В.С. Овчинского*

ООО «Научно-издательский центр ИНФРА-М»
127214, Москва, ул. Полярная, д. 31В, стр. 1
Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29
E-mail: books@infra-m.ru http://www.infra-m.ru

Подписано в печать 10.09.2021.
Формат 60×90/16. Бумага офсетная. Гарнитура Newton.
Печать цифровая. Усл. печ. л. 39,38.
Тираж 400 экз. Заказ № 00000

ТК 766458-1831932-100921

Отпечатано в типографии ООО «Научно-издательский центр ИНФРА-М»
127214, Москва, ул. Полярная, д. 31В, стр. 1
Тел.: (495) 280-15-96, 280-33-86. Факс: (495) 280-36-29