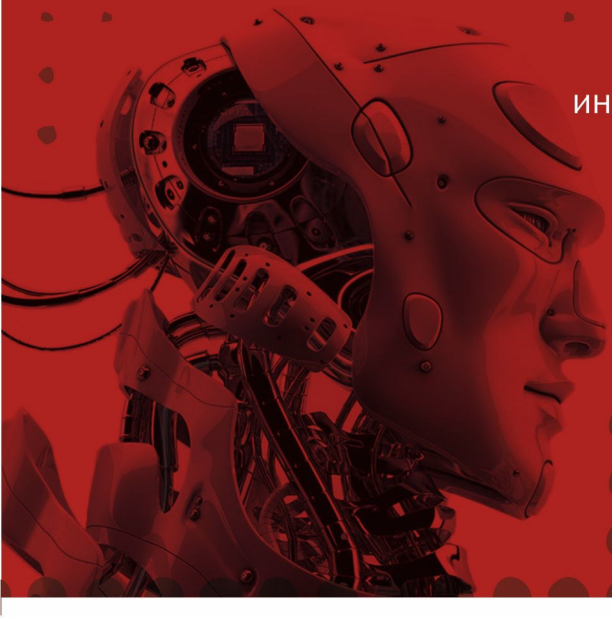
УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ЧТЕНИЯ НА АЛТАЕ



Проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий

Выпуск XV

Министерство науки и высшего образования РФ
Алтайский государственный университет

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ И КРИМИНАЛИСТИЧЕСКИЕ ЧТЕНИЯ НА АЛТАЕ

ВЫПУСК XV

Проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий

Сборник научных статей

Барнаул
Издательство
Алтайского государственного
университета
2018

УДК 343
ББК 67.410.2+67.52
У261

Ответственные редакторы:

С.И. Давыдов, заведующий кафедрой уголовного процесса и криминалистики, доктор юридических наук;

В.В. Поляков, доцент кафедры уголовного процесса и криминалистики, кандидат юридических наук.

У Уголовно-процессуальные и криминалистические чтения на
261 Алтае: проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2018. – Вып. XV.- 228 с.

ISBN 978-5-7904-2331-4

В сборник включены статьи участников тематической XVII Всероссийской научно-практической конференции «Уголовно-процессуальные и криминалистические чтения на Алтае», посвященной проблемам и перспективам противодействия преступлениям, совершаемым с применением информационных технологий. В статьях исследуются теоретические и практические вопросы раскрытия и расследования преступлений, совершаемых с применением информационных технологий; применение новых информационных технологий в уголовно-процессуальной и криминалистической деятельности; криминалистические, уголовно-правовые и криминологические возможности предупреждения преступлений, совершаемых с применения информационных технологий; международное сотрудничество в сфере противодействия высокотехнологичным преступлениям, совершаемым с применением современных информационных технологий.

Сборник издается в рамках поддержанного РФФИ научного проекта 16-33-01160-ОГН.

ISBN 978-5-7904-2331-4

СОДЕРЖАНИЕ

Т.А. Алексеева,
преподаватель кафедры уголовного права
Западно-Сибирский филиал Российского государственного университета правосудия, г. Томск

Р.Л. Ахмедшин,
д.ю.н., профессор, профессор кафедры криминалистики
Юридический институт Томского государственного университета, г. Томск

В.Л. Юань,
старший преподаватель кафедры уголовно-процессуального права
Западно-Сибирский филиал Российского государственного университета правосудия, г. Томск

ИССЛЕДОВАНИЕ ЛИЧНОСТИ ОБВИНЯЕМОГО ПОСРЕДСТВОМ АНАЛИЗА МАТЕРИАЛА СОЦИАЛЬНЫХ СЕТЕЙ

Основные формы отражения личностных характеристики в сведениях, размещаемых лицом в социальных сетях. Позиционирование себя как личности возможно посредством использования большого количества способов. С развитием информационных сетевых ресурсов позиционирование себя с помощью социальных сетей стало явлением повсеместным. Без сомнения, одиночество, неосознанно испытываемое современной личностью, предопределяет передачу иным пользователям максимально насыщенной информации о себе. Использование следователем подобной информации в отношении участников расследования стало тактически обязательным. Игнорирование подобной информацией кроме как вопиющей некомпетентностью исследователя назвать нельзя.

Сведениями, несущими информацию о личности, выступают:

- подбор музыкальных композиций, анализ ритмики которых характеризует эмоциональную сферу автора подборки, а смысловая составляющая – область актуальных ценностных сфер (карьера, отношения, статус, признание и пр.);
- подбор фотографий, анализ содержания которых демонстрирует области, в которых человек не испытывает уверенность (область социальных достижений, область финансового статуса, область межличностных отношений), поэтому посредством которых

пытается транслировать окружающим мысль об успешности в данной сфере;

- подбор сообществ, анализ деятельности которых демонстрирует область интересов человека, сферу его комфортного общения, уровень интеллектуального развития и способности к социализации в конкретной социально-психологической группе;
- совокупность документов, наглядно иллюстрирующих трудовую, учебную, производственную деятельность автора аккаунта социальной сети;
- особенности статусов, иллюстрирующих истероидную (сверхдемонстративную) составляющую личности автора, его представлений о том, что наличие определенных сильных свойств, благих пожеланий, отказа в восприятии чего-либо способно помочь в решении текущих актуальных для лица проблем;

Анализ имени пользователя в социальных сетях. «Не быть, а казаться» - эту фразу можно назвать лозунгом социальных сетей. Любую текстовую информацию в социальных сетях необходимо воспринимать не столько буквально, сколько через призму символьного значения. Человек, действуя в рамках своего психологического типа, оставляет на странице или посте ту информацию, которая наиболее концентрированно характеризует его психологические особенности.

Рассмотрим некоторые примеры, как сведения, указанные в социальных сетях, могут охарактеризовать саму личность, в том числе и личность преступника.

1. Имя пользователя или Nickname.

Создание любой страницы в социальной сети начинается с указания имени пользователя, то есть уже на данном этапе человеку предоставляется возможность сохранения своего настоящего имени или выбора нового.

Указание настоящего имени и фамилии характеризует человека, как сформировавшеюся личность, принимающего себя таким, какой есть, понимающим и принявшим свое место в жизни.

Понимая, что примеров настоящего имени будет большинство, более подробно рассмотрим варианты измененных имен. Наиболее распространенный вариант – это частичное изменение имени пользователя. Примером может быть указание имени и отчества, как попытка придать солидность и вызвать серьезное отношение к своей персоне. К этой же группе относится указание настоящего имени, но измененной или другой фамилии, что помимо присутствия желания «спрятаться» от своих прошлых знакомых, может трактоваться как

некоторая инфантильность, отторжение своей личности, наделение себя желаемыми качествами в интернет-пространстве, соотнесение себя с другим человеком – например, присваивание себе фамилий известных людей, персонажей или прописывание фамилии в форме имени любимого человека (последнее в большей степени касается лиц женского пола). Кроме того, это способ привлечения внимания к своей персоне, особенно в случае выбора двойных или вычурных фамилий, при условии, что они не соответствуют реальным.

Второй вариант – это замена имени и фамилии на другие слова. В данном случае, трактовать выбранные слова нужно через их символьное значение. Например, «Босс», «Император» - превосходство, главенство; «Братишкин» - открытость, легкость заведения новых контактов; «Стрела» - жестокость, целеустремленность; «Крутой» - желание утвердиться в глазах других; «Ухо» - отражение детских комплексов и т.д.

Третий вариант – указание населенного пункта (поселка, города, страны) вместо имени или фамилии, что говорит о необходимости ощущения принадлежности к определенному сообществу, соотнесения себя с группой людей, объединенных местом рождения или местом жительства.

2. Формулирование хештегов (хэштег, хэш-тег).

Хештег – это короткое ключевое слово (или несколько слов), которое обеспечивает поиск по теме или содержанию, используется, как правило, при опубликовании новости или поста в социальной сети. Хештег может быть представлен лаконично, в виде слова, локации, точно определять место или событие, тем самым подчеркивая факт принадлежности субъекта к событию. Подобные хештеги подчеркивают значимость самого события или факт нахождения человека в определенном месте, характеризуют личность, как эмоционально сдержанную, стабильную, стремящуюся к объективности, попытка подчеркнуть насыщенность жизнь событиями.

Напротив, содержание в хештегах личной оценки, местоимения «я», описание эмоций свидетельствует о желании человека получить одобрение со стороны общества, жажда отклика других пользователей, попытка показать испытываемые эмоции.

3. Использование смайликов и эмоджи, которые непосредственно не являются текстовой информацией, но сопровождают написание сообщения в любой социальной сети. В первую очередь они могут указать на возраст автора текста, так как наиболее часто используются подростками, людьми молодого

возраста. Кроме того, можно предположить, что у людей, использующих большое количеством смайликов, имеются некоторые проблемы с выражением эмоций, когда поставить картинку проще, чем описать чувства словами. Важно отметить, что использование смайликов и эмоджи является, в некотором роде, «культурой» написания сообщения в социальных сетях, подчеркивает готовность подстроиться под определенную группу, манеру общения, желание быть как большинство.

Выявление биографических фактов путем оценки фотоснимков на странице обвиняемого в социальных сетях. Современные результаты научных исследований, посвященные проблемам изучения личности посредством анализа страницы в социальной сети [1. С.193; 2. С. 136-137; 3. С. 651, 656-658; 4. С.439; 5. С. 5-11], наглядно доказывают, что криминалистически значимая информация об обвиняемом, содержащаяся в добавленном им на свою страницу контенте способна вывести на знание его психологических свойств, что обеспечит результативность подготовки к допросу в рамках решения криминалистических задач расследования преступлений. На этапе изучения личности обвиняемого существенное преимущество дает получение сведений о фактах из его биографии, поскольку именно на основе анализа биографических фактов можно составить наиболее полный, точный и детальный образ об обвиняемом [6. С. 88-93, 240-241], в том числе выявить значимые психологические черты и определить его психологический тип, при этом даже не имея опыта личного контакта с ним.

Среди блоков пользовательского контента, доступного гостям на страницах в социальных сетях, обычно выделяются основные сведения о самом пользователе (личная информация), сохраненные аудио- и видеофайлы, текстовые сообщения, комментарии, посты, а также фотоснимки, в т.ч. сгруппированные по альбомам. Достаточно информативный блок информации об обвиняемом - это его фотоснимки, поскольку подавляющее большинство социальных сетей ориентированы, в первую очередь, на предоставление пользователям возможности выкладывать изображения, которые могут сопровождаться текстовыми сообщения (к примеру, такая функция широко реализована в Instagram, «В контакте», «Одноклассники» и др.). Проблема изучения личности обвиняемого на основе анализа фотоснимков, которые он добавил на свою страницу, заключается в отборе тех изображений, которые несут на себе данные непосредственно об обвиняемом, исключая сохраненные фотографии или репосты. Немного иначе обстоят дела с изображениями, которые

он сохранил, выложил или опубликовал в рамках флешмоба, а также проиграв спор, испытание или вызов («челлендж»), поскольку описанные ситуации потенциально могут иметь связь с другими, в т.ч. неизвестными биографическими фактами из жизни обвиняемого, давая возможность выйти на них. Здесь рекомендуется отнести такие фотоснимки к категории «потенциально имеющих выход на связь с биографическими фактами из жизни обвиняемого».

Решение проблемы деления всех изображений по признаку наличия или отсутствия связи с конкретным биографическим фактом из жизни обвиняемого видится в создании двух групп изображений. Для этого все изображения со страницы обвиняемого должны быть скопированы на компьютер исследователя и распределены на две папки, соответствующие двум группам.

Первая группа – это такие изображения, которые не имеют ярко выраженного сведения, на основе которой может быть выявлен биографический факт. Косвенными признаками, указывающими на то, что фотоснимок является посторонним и прямого отношения ни к обвиняемому, ни к его жизни не имеет, являются отсутствие или минимальное количество «лайков», минимальное количество или отсутствие комментариев к фотоснимку, а также отсутствие других фотоснимков, которые по смыслу связаны с этим фотоснимком (особенно, если в дату добавления данного фотоснимка не добавлялись другие фотоснимки). Следует уточнить, что критерий «минимальности» определяется в контексте всех остальных фотоснимков. Скорее всего, если большинство фотоснимков имеют множество «лайков» и комментариев, то не составит труда выявить такие, которые резко будут контрастировать на их фоне.

Вторая группа – это фотоснимки, которые подлежат анализу. Здесь целесообразно руководствоваться тем, чтобы на изображении был либо запечатлен сам обвиняемый (полностью или частично), либо какой-то человек, документ, вещь, связанные с его жизнью.

Далее следует провести смысловую группировку всех изображений, относящихся ко второй группе. Для этого необходимо отыскать такие совокупности фотоснимков, которые сделаны в рамках одного определенного события: к примеру, фотоснимки с выпускного, дня свадьбы обвиняемого или празднования Нового года на корпоративной вечеринке, в котором он принимал участие. Как правило, признаками, указывающими на то, что группа фотоснимков относятся к одному событию, являются единая для них одна дата добавления, тематический альбом, а также общая запечатленная на них обстановка с одними и теми же присутствующими на них лицами,

имеющими на всех фотоснимках одинаковый внешний вид (одежда, стиль, прическа и т.д.).

Заключительным этапом является установление связи между запечатленными на фотоснимках событиями и биографическими фактами из жизни обвиняемого. Развивая результаты ранее проведенных исследований, [5. С. 8], классификация биографических фактов, которые могут отразиться в содержательной части анализируемых фотоснимков может быть следующей:

1. Сведения о семье пользователя. Признаки: как правило, это совместные фотографии с членами семьи, в которых стоит обращать внимание на комментарии (особенно от пользователей с аналогичной фамилией), а также на отмеченных на фотографии людей, если такая функция предусмотрена сервисом данной социальной сети. В некоторых сервисах, к примеру, в «Вконтакте» родители, братья, сестры и дети могут указываться самим пользователем в блоке информации о себе;

2. Сведения о месте жительства и жилищных условиях пользователя. Признаки: наличие фотографий, в которых полностью или частично запечатлена домашняя обстановка. Как правило, если большинство фотографий у него снято в каком-то определенном помещении, то чаще всего он в нем живет. Важно установить связь между различными фотографиями, на которых запечатлена какая-то обстановка, поскольку часть из них могут быть сделаны в разных комнатах одной и той же квартиры, в которой живет пользователь. Сюда также относятся фотографии, сделанные в районе его жилого дома, что позволит установить, в каком районе города он проживает;

3. Сведения об окружении пользователя. Признаки: наличие совместных фотографии с одногруппниками, коллегами, друзьями. Здесь также, как и в случае с семейными фотографиями, следует обращать внимание на комментарии и отмеченных на фотографии людей;

4. Сведения о взглядах пользователя. Признаки: фотографии из учреждений соответствующей религиозной и политической направленности, с различных тематических мероприятий, изображения с характерными символиками, фотографии пользователя в соответствующих одеждах, аксессуарах, атрибутикой и т.п.;

5. Сведения об интересах пользователя. Признаки: фотографии с различных мероприятий, изображения и картинки из фильмов, аниме, мультфильмов, игр, фотографии известных людей и т.д.;

6. Сведения о способностях пользователя. Признаки: наличие фотографий, на которых изображены продукты его творческой

деятельности, награды, кубки и медали, свидетельствующие о его спортивных достижениях, фотографии, на которых изображен пользователь, выполняющий определенную деятельность, если нет оснований полагать, что фотография постановочная;

7. Сведения о деятельности пользователя. Признаки: фотографии с мест учебы и(или) работы, дипломы, сертификаты и грамоты, связанные с его учебой или работой, а также связанные с общественной и политической жизнью документы, аксессуары, награды, медали и атрибутика и др.

В исходном виде цепочка методики выявления биографических фактов путем оценки фотоснимков на странице обвиняемого в социальной сети будет иметь трехстадийную структуру и выглядеть следующим образом: техническая группировка (задача: сбор всех фотоснимков, имеющих потенциальный выход на биографические факты из жизни обвиняемого) - смысловая группировка (задача: распределение фотоснимков по группам, в зависимости от их общей, единой связи с одним определенным событием из жизни обвиняемого) - обнаружение связей (задача: выявление взаимосвязей между фотоснимками и определенной группой биографических фактов из жизни обвиняемого). Описанная методика призвана послужить в качестве одного из инструментов оптимального сбора криминалистически значимой информации о личности обвиняемого путем анализа его страниц в социальных сетях для решения криминалистически значимых задач в рамках расследования уголовных дел.

Список литературы

1. Садыгова Т.С. Социально-психологические функции социальных сетей. / Т.С. Садыгова. // Вектор науки Тольяттинского государственного университета. Педагогика, психология. 2012. №3 (10). С. 192–194.

2. Шаповаленко А.А. Активность обвиняемого социальной сети (на примере vk.com) и особенности личностного самоопределения в юности. / А.А. Шаповаленко. // Педагогическое образование в России. 2013. № 4. С. 133–138.

4. Коршунов А. Анализ социальных сетей: методы и приложения. / А. Коршунов, И. Белобородов, Н. Бузун. // Труды Института системного программирования РАН. 2014. №1 (26). С. 439–456.

5. Алексеева Т.А. Основные подходы к содержанию криминалистического анализа личности в социальных сетях. / Т.А.

Алексеева, Р.Л. Ахмедшин, В.Л. Юань // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействия киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. – Барнаул: Издательство Алтайского университета, 2017. Вып. XIV. С. 5-11.

6. Ведерников, Н.Т. Избранные труды. Том 1. / Н.Т. Ведерников. – Томск: Издательство Томского университета, 2009. – 250 с.

Ю.А. Андриенко,
старший следователь по особо важным делам следственной части Главного следственного управления Главного управления МВД России по Алтайскому краю, г. Барнаул

ОТДЕЛЬНЫЕ ВОПРОСЫ КРИМИНАЛИСТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ

В сентябре текущего года в отечественных СМИ получила огласку новость о том, что Федерация профсоюзов Великобритании вышла с инициативой о сокращении рабочей недели до четырех дней, мотивируя это широким использованием в труде новых технологий, которые могут позволить сотрудникам различных организацийменьше работать при сохранении прежней производительности и заработной платы [1]. В указанном предложении существует значительная доля логики, поскольку внедрение технологических инноваций, продуктов информационных технологий в различные отрасли человеческой деятельности призвано не только для получения новых знаний, совершения научных открытий, но и для их практического применения, облегчения труда человека, для оптимизации расхода человеческих ресурсов, прежде всего, времени и сил, необходимых для решения задач, стоящих перед конкретным индивидом и обществом в целом. Если о введении четырехдневной рабочей недели у сотрудников российских правоохранительных органов говорить всерьез в настоящее не приходится в силу особенностей возложенных на них задач, выражающихся в первую очередь в необходимости непрерывного обеспечения безопасности общества и государства от

преступных посягательств, то вопрос острой необходимости введения продуктов новых технологий, в том числе информационных и телекоммуникационных, заслуживает особо внимания.

Современная преступность, особенно в ее организованных формах, широко применяет достижения науки, продукты цифровых технологий при осуществлении разного рода незаконной деятельности, используя их непосредственно как средство совершения преступлений, так и с целью конспирации и обеспечения своей безопасности. Мошенничества, сбыты наркотических средств, акты экстремизма и терроризма и многие другие преступления, совершаемые с использованием информационных и телекоммуникационных технологий, уже на протяжении нескольких лет регулярно бросают вызовы безопасности личности и общества.

Следователь, будучи должностным лицом, осуществляющим предварительное расследование и направляющим его ход, принимающим итоговое решение по делу, безусловно, является важнейшим участником уголовного судопроизводства на его досудебной стадии. Решая задачи всестороннего, полного и объективного исследования обстоятельств совершенного преступления, уголовного преследования лиц, его совершивших, следователь находится на передовой линии борьбы с преступностью и защиты прав и законных интересов граждан, общества и государства. Именно поэтому необходимым ответом на вызовы технологически развивающейся преступности должно являться актуальное и современное криминалистическое обеспечение предварительного расследования, которое бы позволило следователю эффективно решать стоящие перед ним задачи процессуального, тактического и организационного характера.

Вышесказанное подтверждается и положениями ч. 4 ст. 6.1 УПК РФ, согласно которым обстоятельства, связанные с организацией работы органов дознания, следствия, прокуратуры и суда не могут приниматься во внимание в качестве оснований для превышения разумных сроков осуществления уголовного судопроизводства. Применительно к деятельности следователя это означает, что он должен в кратчайшие сроки произвести качественное расследование дела и принять по нему законное и обоснованное решение, невзирая на любые трудности, в том числе касающиеся организации его работы, ее материального, технического и технологического обеспечения.

Несмотря на несомненную важность и значимость следственной работы, необходимо признать, что «арсенал» современного следователя не всегда соответствует требованиям времени.

Значительная часть элементов работы по расследованию уголовных дел остается практически неизменной на протяжении нескольких десятков лет. Так, многие следственные работники с легкостью узнают себя в главном герое фильма «Допрос», снятого в 70-е годы прошлого века, повествующего о жизни и работе советского следователя, роль которого исполнил А. Калягин. В данной ленте главный герой предстает как загруженный работой человек с хронической усталостью, все мысли которого занимают расследуемые уголовные дела и процессуальные сроки. Мало кто будет спорить, что портрет среднестатистического российского следователя может быть описан примерно так же.

Действительно, расследование и направление в суд уголовных дел по-прежнему нередко сопровождаются большой тратой личных временных ресурсов и сил. Несомненно, зачастую сама специфика работы требует от следователя сверхусилий, например, при производстве следственных действий по задержанию подозреваемых или проведению обысковых мероприятий, что нередко происходит в ночное время. Даже при самом передовом техническом оснащении кардинальным образом облегчить или упростить подобную работу вряд ли получится. Вместе с тем некоторые трудности в работе следователя в значительной степени связаны исключительно с вопросами организационного характера, а также проблемами применения некоторых продуктов современных технологий и потенциально могут быть решены.

В связи с изложенным, представляется целесообразным выявить и проанализировать некоторые из обозначенных выше вопросов криминалистического обеспечения предварительного расследования, предпринять попытку отыскания путей их решения, и на этой основе определить общие направления для оптимизации процесса осуществления предварительного расследования.

Не секрет, что значительную часть рабочего времени следователя занимает получение криминалистически значимой информации, которая позволяет детально установить событие преступления, виновность лица, обстоятельства, характеризующие личность обвиняемого и другие важные сведения. Это достигается не только посредством допросов участников уголовного судопроизводства или осмотров вещественных доказательств, но и путем обращения к различным базам данных, имеющимся в распоряжении правоохранительных органов, а также взаимодействия с другими организациями, как государственными, так и частными.

Подобная необходимость возникает, например, в процессе установления времени, места, способа, средств совершения преступления и других признаков его объективной стороны, когда следователю необходимо получить сведения об имущественном и материальном положении обвиняемого, использовавшихся им при совершении преступлений абонентских номерах, банковских счетах, транспортных средствах, объектах недвижимости. С целью уточнения места совершения преступления у следователя зачастую возникает необходимость в запросе в соответствующих органах информации о верных адресах зданий, наименованиях дорог, улиц и других объектов, сведений о географических координатах и получении других сведений. При выполнении требований п. 3 ч. 1 ст. 73 УПК РФ путем сбора исчерпывающего характеризующего материала в отношении обвиняемого следователю необходимо выяснить и приобщить к уголовному делу в виде соответствующих документов сведения о личности лица, его семейном положении, наличии детей, образовании, трудоустройстве, прежних судимостях, административных правонарушениях, состоянии здоровья, воинской обязанности, наличии водительского удостоверения и т.д.

В отечественной науке деятельность следователя по получению вышеперечисленной и другой криминалистически значимой информации нередко именуется *информационным обеспечением предварительного расследования*. Так, Е.Н. Паршина определяет информационное обеспечение предварительного расследования как целенаправленную деятельность должностных лиц, уполномоченных осуществлять предварительное расследование, подразделений и служб органов внутренних дел, направленную на удовлетворение информационных потребностей субъектов расследования, а также создание оптимальных условий для эффективного использования информации в целях раскрытия и расследования преступлений [2].

Как уже было сказано выше, частично следователь решает вопрос информационного обеспечения путем осуществления разрешенного доступа к различным базам данных. Вместе с тем, объем сведений в указанных базах данных весьма ограничен, и в остальном получение необходимой информации сводится к направлению запросов в соответствующие организации. Данный процесс позволяют ускорить различные современные средства связи, в частности, сервисы электронного документооборота (в том числе электронной почты), посредством которых и осуществляется получение необходимых сведений. Однако практика показывает, что не все организации могут исполнять запросы подобным образом, что, как правило, связано с

отсутствием соответствующего технического оснащения или установленным исключительно нарочным порядком обмена корреспонденцией. В этом случае процесс получения необходимых сведений может занять от нескольких дней до месяца, а в ряде случаев и более продолжительный период времени. В условиях общего требования окончания предварительного следствия в срок, не превышающий 2 месяцев, подобные временные затраты следует признать недопустимыми. Кроме того, зачастую оперативное получение нужной информации необходимо для назначения судебных экспертиз, установления и допроса свидетелей, владеющих ценными сведениями, и любое промедление может повлечь утрату доказательств по уголовному делу.

Представляется, что для преодоления изложенных выше проблем существует несколько путей. По мнению автора статьи, одним из эффективных способов оптимизации процесса доказывания в рассматриваемом аспекте явилось бы значительное расширение баз данных, которыми в своей деятельности пользуется отечественный следственный аппарат. На первоначальном этапе в подобные базы данных могли бы быть включены наиболее востребованные в процессе расследования данные таких государственных органов как, например, Министерство здравоохранения (в частности, сведения о состоянии лица на учете в психиатрических и наркологических диспансерах), Росреестр, органы судебной власти, Федеральная налоговая служба, Федеральная служба судебных приставов, Роскомнадзор и ряд других органов государственной власти. В дальнейшем было бы целесообразно рассмотреть вопрос о включении в вышеуказанные базы данных сведений, имеющихся в распоряжении сотовых операторов, кредитно-финансовых учреждений, организаторов распространения информации (компаний – владельцев интернет-сайтов, мессенджеров, социальных сетей и т.д.).

Оперативное получение следователем указанных сведений позволило бы существенным образом ускорить процесс информационного обеспечения предварительного расследования, придать ему более активный и наступательный характер и значительно ускорить процесс доказывания.

Противники вышеописанной идеи в первую очередь выскажут опасения о возможных злоупотреблениях со стороны работников правоохранительных органов при осуществлении доступа к указанным данным, выражающихся в их недобросовестном использовании. В качестве контраргумента можно сказать, что, во-первых, при организации подобных банков данных целесообразно предусмотреть

авторизованный доступ к их информационным базам, при осуществлении которого сотруднику будет необходимо указать причину обращения, номер уголовного дела (материала проверки), в рамках которого запрашивается информация, и другие сведения, позволяющие сделать использование базы данных максимально прозрачным и исключающим любые неправомерные действия. Во-вторых, при наличии в уголовно-процессуальном законе требований о недопустимости влияния организационных сложностей в работе следователя на разумный срок уголовного судопроизводства органам предварительного расследования должен быть предоставлен настолько мощный криминалистический инструментарий, который бы позволил свести к минимуму возможность возникновения проблем в организации расследования уголовного дела. И, наконец, в-третьих, вопрос возможного злоупотребления получаемой следователем информацией в процессе расследования относится скорее к проблеме надлежащего кадрового обеспечения следственных органов, решение которой не входит в перечень задач, стоящих перед следователями и никоим образом не зависит от них.

В любом случае, несмотря на свой дискуссионный характер, рассмотренный выше вопрос является предельно актуальным и злободневным и заслуживает дальнейшего внимания, обсуждения и проработки.

Другим важным и перспективным направлением оптимизации информационного обеспечения предварительного расследования является развитие взаимодействия следственных органов со сторонними организациями с целью получения нужной информации посредством информационно-телекоммуникационных сетей. Как уже говорилось выше, в процессе деятельности по информационному обеспечению расследования следователь контактирует с множеством государственных и частных организаций, однако лишь в некоторых из них с целью оперативного обмена информацией созданы условия для приема и отправки корреспонденции в электронном виде (например, ПАО Сбербанк, Росреестр).

Представляется, что устоявшаяся форма запросов следственных органов с наличием печати и подписи инициатора, требуемая большинством организаций, является устаревшей и вполне может быть заменена на электронный вид документа, полученный посредством информационно-телекоммуникационных сетей и снабженный электронной подписью. Определенность в решении данного вопроса могла бы быть внесена наличием соответствующих норм УПК РФ, однако глава 56 уголовно-процессуального закона,

регулирующая порядок использования электронных документов в уголовном судопроизводстве, таких положений не содержит.

В заключение следует сказать, что необходимость использования продуктов цифровых технологий в каждодневной работе следователя ни в коем случае нельзя считать «реверансом» научно-техническому прогрессу или проявлением технократии, это – требование времени, игнорирование которого непозволительно. В то время как современные преступники используют в своей незаконной деятельности возможности работы на внешних серверах посредством удаленного доступа, разрабатывают для использующихся программ сложные ключи шифрования, совершают финансовые операции в криптовалюте, следователи продолжают посредством нарочного отправления и получения собирать нужную информацию, месяцами ожидают ответы на запросы, зачастую не имеют на рабочем месте доступа в интернет. Такое положение вещей следует признать даже не «вчерашним», а «позавчерашним» днем. Очевидно, что именно по пути внедрения информационных технологий должно, и, по всей видимости, будет развиваться криминалистическое обеспечение предварительного расследования. От того, насколько интенсивно будет происходить этот процесс, зависит дальнейшая возможность следователя осуществлять эффективное, быстрое и полное расследование.

Список литературы

1. В Великобритании предложили ввести 4-дневную рабочую неделю // URL: https://rg.ru/2018/09/10/v-velikobritanii-predlozhili-vvesti-4-dnevnuiu-rabochuiu-nedeliu.html (дата обращения: 02.12.2018).

2. Паршина, Е. Н. Проблемы информационного обеспечения и защиты информации в предварительном расследовании преступлений : автореф. дис. ... канд. юрид. наук : 12.00.09 / Паршина Елена Николаевна.– Ижевск, 2004. – 23 с.

А.А. Балашова,
адъюнкт кафедры управления органами расследования преступлений Академия управления МВД России, г. Москва

КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ И ЕЕ РОЛЬ В УГОЛОВНОМ ПРОЦЕССЕ РОССИИ

В настоящее время, в связи с потоком противоправных деяний, связанных с электронными носителями информации, совершаемыми в информационной сфере, компьютерная информация часто выступает предметом преступления.

Для начала уточним, что же такое компьютерная информация, которая кстати является разновидностью электронной информации, определение которой содержится в Уголовном кодексе Российской Федерации. Под компьютерной информацией следует понимать сведения, сообщения, данные, которые представлены в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [1].

Специфика преступлений, связанных с электронной информации обусловлена использованием как новых технологий, так и необходимостью обладания определенным уровнем специальных познаний, но в настоящее время в сети Интернет присутствуют определенного рода программы, которые предназначены для совершения несанкционированных действий с названной информацией, а так же инструкции по их применению [2].

Исследователи-процессуалисты также предлагают следующую характеристику компьютерной информации: [3]

1) она объёмна и быстро обрабатываема;

2) она очень легко и, как правило, бесследно уничтожаема;

3) она обезличена, т.е. между ней и лицом, которому она принадлежит, чаще всего нет жесткой связи;

4) она может находиться лишь на машинном носителе (дискете, магнитной ленте, лазерном диске, полупроводниковых схемах и др.), в самой ЭВМ (оперативной памяти - ОЗУ);

5) она может создаваться, изменяться, копироваться, применяться (использоваться) только с помощью ЭВМ;

6) она легко передаётся по телекоммуникационным каналам связи компьютерных сетей, причём практически любой объём информации можно передать на любое расстояние;

7) она относительно проста в пересылке, преобразовании, размножении; при её изъятии, в отличие от изъятия вещи, она легко

сохраняется в первоисточнике; доступ к одному и тому же файлу, содержащему информацию, могут одновременно иметь несколько пользователей.

Компьютерная информация в процессе доказывания обладает признаками документов и именно поэтому ее необходимо и рассматривать в качестве документов. Она может быть доведена как от органов государственной власти, так и от органов местного самоуправления, кроме того, ее можно получить от общественных объединений и организаций, учреждений, предприятий, а так же должностных лиц и граждан. Они в обязательном и в установленном порядке должны предоставлять запрашиваемые документы или копии этих документов. Та информация, которая запечатлена на магнитном носителе, требует необходимости признания ее доказательством, но это будет возможно только в том случае если полученные сведения, будут служить средствами для обнаружения преступления и иметь значение для установления обстоятельств уголовного дела. В обязательном порядке, компьютерная информация приобретает значение доказательств, когда она полностью отвечает требованиям допустимости. Но в любом случае, если будет выявлен факт получения доказательств с нарушением требований УПК РФ, то они будут являются недопустимыми, и они не будут иметь юридической силы а так же положены в основу обвинения. Несмотря на это, компьютерную информацию необходимо различать от иных документов и от вещественных доказательств. Так, например, Зигура Н.А. описывает это различие следующим образом, она считает, что основания для разграничения компьютерной информации от иных документов могут быть следующие:

- по механизму формирования – в данном случае, источник доказательств применительно к иному документу это сам автор данного документа, тогда как компьютерная информация может быть создана при помощи алгоритма, который будет задан программой;

- по среде существования – если иной документ будет предназначен для обработки людьми, и среда существования является аналоговой. В данном случае компьютерная информация обрабатывается определенными техническими объектами или программами средствами.

- по привязке к носителю - иной документ имеет жесткую привязку к материальному носителю. Компьютерная информация такой привязки не имеет, потому что материальный носитель, в

отличие от иного документа, может быть использован множество раз для записи любой информации, а не однократно.

- по признаку воспроизведения - иной документ непосредственно будет восприниматься органами чувств человека. Компьютерная информация воспринимается только объектом цифровой среды – иначе говоря техническим или программным средством [4].

Теперь необходимо сделать акцент на основных видах компьютерной информации, содержащейся на электронных носителях:

1. Электронный документ - это та документированная информация, которая представлена в электронной форме, в виде пригодном для восприятия человеком, с использованием электронных вычислительных машин;
2. Электронное сообщение - информация, которая может быть передана или получена пользователем информационно-телекоммуникационной сети, доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети "Интернет»;
3. Сайт в сети «ИНТЕРНЕТ» - определенная совокупность программ для электронных носителей и иной информации, которая содержится в информационной системе;
4. Доменное имя - обозначение символами, предназначенное для адресации сайтов в сети "Интернет" в целях обеспечения доступа к информации, размещенной в сети "Интернет";
5. Сетевой адрес - идентификатор в сети передачи данных, который определяет оказание телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему.

Нельзя забывать и о классификации, которая важна для разработки средств, а так же приемов, методов, фиксации, осмотра, изъятия, исследования компьютерной информации, а также возможность использовать данную информацию при выявлении, расследовании преступлений и в дальнейшем при судебных разбирательствах по уголовным делам.

Мы хотим остановиться на следующих основаниях для классификации компьютерной информации, наиболее важных и приемлемых по нашему мнению:

1). По связи с событием преступления:

- компьютерная информация, которая служила орудием совершения преступления;

- компьютерная информация, которая сохранила на себе следы преступления;

- компьютерная информация, на которую были направлены преступные действия;

- иная компьютерная информация, которая устанавливает наличие или отсутствие обстоятельств,

- подлежащих доказыванию при производстве по уголовному делу, а также иных обстоятельств, имеющих значение для уголовного дела.

Установление объективной действительности будет являться значением классификации по указанному основанию и соответствовать цели уголовно-процессуального доказывания. При расследовании уголовного дела подлежит доказыванию событие преступления (время, место, способ и иные обстоятельства совершения преступления, о чем говорится в ст. 73 ч. 1 п. 1 УПК РФ). Событие преступления и виновность конкретного лица в совершении преступления - эти основные элементы предмета доказывания.

2). Классификация по происхождению включает в себя следующие элементы:

- компьютерная информация, созданная (внесенная) пользователем;

- компьютерная информация, созданная аппаратными и программными средствами.

В данном случае механизм образования компьютерной информации лежит в основании данной классификации. Способ исследования информации так же различен. Просматривается некоторая аналогия между механизмом образования компьютерной информации первого вида и личными доказательствам и между компьютерной информацией второго вида и вещественными доказательствам.

3). Классификация по типу данных

- текстовая информация;
- базы данных;
- графическая информация;
- мультимедийная;
- программы для ЭВМ.

Значение данной классификации состоит в том, что с при помощи разнообразных программ, отображаются и исследуются различные типы данных. Отличными друг от друга являются подходы и методы исследования этих типов данных. Например, при исследуя

базы данных необходимо учитывать возможность их распределенного хранения.

Таким образом, очевидно, что на компьютерную информацию может быть распространен режим вещественного доказательства по уголовному делу.

Компьютерная информация, которая непосредственно будет обладать значением доказательства в качестве фактических данных, а также ее носитель, могут быть закреплены только в предметной форме либо путем изъятия самого носителя, либо копирования компьютерной информации на другой цифровой носитель.

Хочется сделать вывод, что, что при проведении следственных действия, в момент проведения которых будет производиться такое действие как - осмотр или изъятие компьютерной информации и техники, необходимы будут решения определенных специальных задач, таких как установление наличия и обеспечение полноты и адекватности информации, которая изымается. В связи с тем, что на сегодняшний день не существует специальная техника, методика для исследования компьютерной информации в том месте, где проводятся следственные действия, такие исследования целесообразно проводить в лабораторных условиях. Компьютеры должны подлежать изъятию с обязательным условием сохранения имеющейся компьютерной информации в первоначальном виде и в дальнейшем обеспечения ее сохранности во время транспортирования изъятых компьютерных средств.

Список литературы

1. Уголовный кодекс Российской Федерации: принят Федеральным законом от 13 июня 1996 г. N 63-ФЗ // Собрание законодательства Российской Федерации. 1996. N 25. Ст. 2954

2. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации: утв. Генеральной прокуратурой Российской Федерации. URL: http://www.genproc.gov.ru (дата обращения: 15.04.2018).

3. Шарков А.Е. Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации: дис. ... канд. юрид. наук. - Ставрополь, 2004. - С. 30.

4. Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. ... канд. юрид. наук. Челябинск, 2010. 20 с.

С.В. Баринов,
к.ю.н., доцент кафедры гуманитарных и социально-экономических дисциплин
Филиал ВУНЦ ВВС «ВВА имени проф. Н.Е. Жуковского и Ю.А. Гагарина» в г. Сызрани

ОСОБЕННОСТИ ДОКАЗЫВАНИЯ ПРЕСТУПНЫХ НАРУШЕНИЙ НЕПРИКОСНОВЕННОСТИ ЧАСТНОЙ ЖИЗНИ, СОВЕРШАЕМЫХ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ ИНТЕРНЕТ

К группе преступных нарушений неприкосновенности частной жизни нами относятся запрещенные в ст.ст. 137, 138 и 139 УК РФ под угрозой наказания общественно опасные виновно совершенные деяния, посягающие на гарантированные Конституцией РФ права на личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений, а также на неприкосновенность жилища [1, с. 5].

Рассмотрение преступных нарушений неприкосновенности частной жизни как отдельной группы преступлений представляется целесообразным в целях выявления общих закономерностей их совершения, изобличения и привлечения виновных к ответственности, разработки комплекса мер по предотвращению преступлений, а также для решения других актуальных задач борьбы с преступностью в рассматриваемой сфере [2, с. 7].

Выделенные в группу преступных нарушений неприкосновенности частной жизни составы преступления исследователями относятся к категории информационных преступлений [3, с. 166]. Из этого следует, что предметом преступления является информация – сведения, составляющие личную или семейную тайну лица.

Предметом преступных посягательств на неприкосновенность частной жизни часто становятся фото- и видеоизображения человека. Часто такие изображения демонстрируют интимные стороны личной жизни. Следует также отметить, что до 10% таких изображений в ходе расследования преступлений признавались порнографическими, а деяния дополнительно квалифицировались по ст. 242 УК РФ (незаконное изготовление и оборот порнографических материалов или предметов).

Криминогенная ситуация в сфере неприкосновенности частной жизни сегодня характеризуется тем, что значительное число

преступных деяний совершается в киберпространстве. Исследователями отмечается, что ресурсы информационно-телекоммуникационной сети «Интернет» могут быть использованы не только для совершения высокотехнологичных преступлений, но и как платформа для размещения информационных объектов, которые впоследствии, при соблюдении процессуальных требований, будут иметь доказательственное значение в рамках расследования конкретного уголовного дела [4, с. 109].

А.Л. Осипенко выделяет следующие особенности, характерные для нарушений, совершаемых в глобальных компьютерных сетях: повышенная скрытность совершения преступления, обеспечиваемая спецификой сетевого информационного пространства (развитые механизмы анонимности, сложность инфраструктуры и т. п.); трансграничный характер сетевых преступлений, при котором преступник, объект криминального посягательства, потерпевший могут находиться на территориях разных государств; особая подготовленность преступников, интеллектуальный характер преступной деятельности; нестандартность, сложность, многообразие и частое обновление способов совершения преступлений и применяемых специальных средств; возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно, возможность объединять относительно слабые ресурсы многих отдельных компьютеров в мощное орудие совершения преступления; многоэпизодный характер криминальных действий при множественности потерпевших; неосведомленность потерпевших о том, что они подверглись преступному воздействию; дистанционный характер преступных посягательств в условиях отсутствия физического контакта преступника и потерпевшего; невозможность предотвращения и пресечения преступлений данного вида традиционными криминалистическими средствами [5].

Способами совершения преступных посягательств на неприкосновенность частной жизни в информационно-телекоммуникационной сети «Интернет» являются:

- незаконное собирание сведений о частной жизни лица, составляющих его личную или семейную тайну;

- незаконное распространение сведений о частной жизни лица, составляющих его личную или семейную тайну;

- нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан.

По доказыванием понимается непосредственная и опосредованная познавательно-удостоверительная уголовно-

процессуальная деятельность уполномоченных уголовно-процессуальным законом субъектов уголовного судопроизводства по собиранию, проверке, оценке и использованию доказательств с целью установления обстоятельств, имеющих значение для законного, обоснованного и справедливого рассмотрения и разрешения уголовного дела [6, с. 227].

Доказывание виновности лица в совершении преступных посягательств на неприкосновенность частной жизни в информационно-телекоммуникационной сети «Интернет» имеет свои особенности.

Перечень обстоятельств, подлежащих доказыванию, закреплен в ч. 1 ст. 73 УПК РФ. При этом нужно иметь ввиду, что исследователями неоднократно поднималась проблема неполноты закрепленного в уголовно-процессуальном законе перечня подлежащих доказыванию обстоятельств. В частности, в нем не отражены такие элементы состава преступления, как объект преступного посягательства, субъект преступления, а также отдельные характеристики объективной стороны и субъективной стороны [7].

При установлении обстоятельств, подлежащих доказыванию, следует учесть их особенности, характерные для преступлений рассматриваемой группы.

Специфику установления имеют место и время совершения преступления. Доступность современных технических средств, имеющих функцию доступа к информационно-телекоммуникационным сетям позволяет совершать преступные нарушения неприкосновенности частной жизни практически из любого места - помещения, автомобиля, метро, на улице. Так, при расследовании уголовного дела по ч. 1 ст. 137 УК РФ, возбужденного в отношении гражданина Ю., было установлено, что распространение сведений, составляющих личную тайну Н. он совершил посредством отправки ее знакомым ММС-сообщений используя мобильный телефон марки «Самсунг» в помещении магазина «Пивасик» [8].

Между отдельными преступными действиями, совершаемыми преступником, может пройти значительный период времени. Показательным примером является уголовное дело по ч. 1 ст. 137 УК РФ, в ходе расследования которого было установлено, что в один из дней марта 2015 г. гражданин К. противоправно скопировал с ноутбука потерпевшей на переносной накопитель информации видеофайлы с аудиовизуальными изображениями эротического содержания с ее участием. Разместил же указанные видеофайлы с

использованием Интернет-ресурса социальной сети «В контакте» преступник 3 апреля 2016 г. [9].

При расследовании преступных нарушений неприкосновенности частной жизни, совершенных в информационно-телекоммуникационной сети «Интернет» важное значение имеют установление:

- содержания информации, явившейся предметом преступного посягательства;
- достоверности информации;
- конфиденциальности информации;
- лица, тайну частной жизни которого содержат сведения;
- незаконности действий с информацией [10].

В связи с тем, что согласно ч. 3 ст. 20 УПК РФ, деяния, предусмотренные ч.1 ст. 137, 138 и 139 УК РФ относятся к делам частно-публичного обвинения, поводом для возбуждения уголовного дела является заявление потерпевшего или его законного представителя.

Потерпевшим по делам рассматриваемой группы преступлений признается физическое лицо, которому в результате преступных действий, нарушающих его личную или семейную тайну причинен физический, имущественный, моральный вред.

Информацию о совершенном преступлении жертва узнает лично (например, из поступивших сообщений об изменении учетных данных в личном кабинете, при невозможности получения доступа к аккаунту и т.д.) или от знакомых (например, о поступившей им информации компрометирующего жертву характера, обращений в их адрес с предложением предоставить такую информацию и т.д.).

В соответствии с ч. 2 ст. 140 УПК РФ основанием для возбуждения уголовного дела является наличие достаточных данных, указывающих на признаки преступления. Если данных, указывающих на признаки преступления в заявлении потерпевшего недостаточно, дознаватель, орган дознания, следователь, руководитель следственного органа вправе провести предварительную проверку и осуществить действия, предусмотренные ч. 1 ст. 144 УПК РФ.

Среди сведений, которые необходимо получить от заявителя:

- где, когда и при каких обстоятельствах запечатлена информация;
- место хранения информации;
- применяемые способы защиты от постороннего доступа;
- перечень лиц, имевших свободный доступ к носителю информации;

- перечень лиц, имевших свободный доступ в помещение, где находился носитель информации;

- давалось ли разрешение кому-либо на производство различных действий с информацией, в какой форме и на каких условиях;

- где в настоящее время находится и в каком состоянии носитель информации;

- имеются ли признаки модификации информации;

- когда и при каких обстоятельствах стало известно о преступлении;

- какие действия совершены заявителем по сохранению следов преступления, установлению лица, получившего доступ;

- информационно-телекоммуникационная сеть (социальная сеть), где зарегистрирован аккаунт;

- IP-адреса, с которых осуществлялся пользователем доступ к аккаунту;

- возможность доступа пользователя к содержимому аккунта после совершения преступных действий;

- сохранность информации;

- когда может быть предоставлен доступ к содержимому аккаунта сотрудникам правоохранительных органов.

Необходимо также установить перечень лиц, сведения о которых содержатся в информации. Впоследствии такие лица могут быть признаны потерпевшими по уголовному делу.

По результатам изучения материалов следственно-судебной практики можно констатировать, что по большинству уголовных дел преступником являлся знакомый жертвы: бывший супруг, сожитель, родственник, сосед, коллега по работе и т.д. Поэтому следует установить факты межличностных конфликтов с участием потерпевшего, возникших в период времени, непосредственно предшествующего совершению преступного посягательства в семье, среди знакомых, в трудовом коллективе. В этой связи в ходе получения первых показаний заявителя по делу возникает возможность приблизительно очертить круг подозреваемых.

Так, потерпевшая по уголовному делу по ч. 1 ст. 138, ч. 1 ст. 272, ч. 1 ст. 137 УК РФ, возбужденному в отношении гражданина К., пояснила, что в начале февраля 2014 года, она зашла на свою страницу в социальной сети имея от знакомого информацию о том, что накануне он видел, что ее страница в 5 часов утра является активной, то есть кто-то от ее имени выходил на ее страницу в социальной сети. Поскольку она этого не делала, то сразу поняла что неизвестный

пользователь «взломал» пароль ее страницы. В настройках своей страницы она увидела, что на ее страницу заходили с другого адреса. Она сразу предположила, что это сделал бывший супруг, чтобы прочитать ее личную переписку [11].

В ходе расследования уголовных дел, возбужденных по фактам нарушений неприкосновенности частной жизни, совершаемых в сети «Интернет», особое значение имеет фиксация визуальной информации.

Местами размещения такой информации являются страницы пользователей социальных сетей, форумы, чаты, сайты знакомств и объявлений, порно-сайты.

По изученным в ходе исследования уголовным делам применялись следующие способы фиксации доказательственной информации из сети «Интернет»: описание, фотографирование и скрин-шоты.

В протоколах осмотров страниц пользователей социальной сети указывались сведения о ее принадлежности, времени ее создания, времени последнего использования, описание содержания конфиденциальной информации и сопутствующих ей текстов.

Установление фактов доступа к содержимому аккаунта и незаконных действий с информацией осуществлялось путем направления запросов оператору, предоставившему доступ к телекоммуникационной сети. В таких запросах истребовалась информация:

- о заключении договора на предоставление телематических услуг связи;
- установочные данные абонента;
- аутентификационные данные (IP-адрес абонента, используемый для доступа к сети Интернет);
- логин и пароль для входа в личный кабинет;
- когда и с какого IP-адреса осуществлялись действия по заведению, модерации, переписке, смене паролей, посещению страницы потерпевшего;
- какому абоненту выделен установленный IP-адрес и где данный абонент зарегистрирован.

Очевидцами совершаемых в информационно-телекоммуникационной сети «Интернет» преступных нарушений неприкосновенности частной жизни могут быть лица, получавшие направленные в свой адрес сообщения, содержащие сведения о частной жизни потерпевшего, либо обнаружившие их в открытом доступе. Кроме описания обстоятельств получения информации,

содержащей сведения о частной жизни потерпевшего, такие свидетели могут охарактеризовать его образ жизни, высказать подозрения в отношении причастности определенных лиц к преступлению, а также об обстоятельствах, способствовавших его совершению.

Так, свидетель по уголовному делу, возбужденному по ч. 1 ст. 137 и ч. 1 ст. 138 УК РФ в отношении гражданина Л. сообщил, что в начале мая 2016 года, точную дату он не помнит, ему на электронную почту пришло письмо. Данное письмо пришло ему с адреса электронной почты знакомой, однако, как он понял, письмо, было написано от имени ее мужа. В указанном письме был текст, с примерным содержанием о том, что посмотрите какая Л. плохая и не заботится о дочке. К сообщению были прикреплены файлы маленьких фотографий, на которых была изображена потерпевшая. Ранее потерпевшая говорила свидетелю, что отношения в семье стали портиться, происходили ссоры с мужем, но на какой почве они происходили ему не известно [12].

При установлении сведений о возможном местонахождении средств совершения преступления, предметов или документов, которые могут иметь значение для уголовного дела, рекомендуется провести обыск.

Обыск - следственное действие, имеющее поисковый характер. При производстве обысков по делам о преступных посягательствах на неприкосновенность частной жизни, совершаемых в информационно-телекоммуникационной сети «Интернет» обычно изымаются:

- персональные компьютеры (планшеты, ноутбуки);
- мобильные телефоны;
- электронные средства хранения информации (флеш-накопители, съемные жесткие магнитные диски, компакт-диски CD-R, CD-RW);
- WiFi-роутеры;
- документы, дневники и различные записи, имеющие значение для расследуемого уголовного дела.

Другими следственными действиями, в ходе которых изымаются средства совершения преступления, предметы или документы, которые могут иметь отношение к преступленному деянию, являются выемка и осмотр места происшествия.

Изъятая в ходе следственных действий компьютерная техника направляется для производства компьютерной технической судебной экспертизы, на разрешение которой ставятся вопросы установления следов посещения страницы сайта «...», имеющей учетную запись «...», следов доступа на почтовый ящик потерпевшего в определенный

период времени, следов изменения пароля доступа к странице сайта «...», следов смены пароля для доступа к почтовому ящику потерпевшего, следов, свидетельствующих о доступе к созданному паролю к почтовому ящику и др.

Криминалистическая характеристика личности преступника, совершающего преступные нарушения неприкосновенности частной жизни в сети «Интернет» позволяет предположить, что типичным преступником является мужчина в возрасте от 17 до 35 лет, житель города, имеющий среднее специальное, незаконченное высшее или высшее образование, владеющий навыками работы с персональным компьютером, активный пользователь сети «Интернет», не женатый, психически неуравновешенный, испытывающий проблемы во взаимоотношениях с противоположным полом. Лица, совершившие преступление ранее не судимы, не имеют устойчивых связей с криминалитетом, не ведут антисоциальный образ жизни [13].

Учитывая приведенную криминалистическую характеристику личности типичного преступника, совершающего преступные посягательства на неприкосновенность частной жизни в информационно-телекоммуникационной сети «Интернет», следует ожидать, что при наличии достаточных доказательств, изобличающих виновного, он займет конструктивную позицию, даст признательные показания, раскается в содеянном, предпримет попытки к устранению ущерба, будет активно содействовать расследованию.

Список литературы

1. Баринов С.В. Проблемы выявления и расследования преступных нарушений неприкосновенности частной жизни. Автореф. ... дис. к.ю.н. Саратов, 2006. 24 с.

2. Баринов С.В. Преступные нарушения неприкосновенности частной жизни как объект криминалистического исследования: учебное пособие. Ульяновск: Зебра, 2017.

3. Крылов В.В. Расследование преступлений в сфере информации. М.: Городец. 1998.

4. Колычева А.Н. Некоторые аспекты фиксации доказательственной информации, хранящейся на ресурсах сети Интернет // Вестник Удмуртского университета. Серия Экономика и право. 2017. Т. 27. вып. 2. - С. 109 - 113.

5. Осипенко А.Л. Сетевая компьютерная преступность: теория и практика борьбы : монография. Омск : Омская академия МВД России, 2009. С. 109-110.

6. Торбин Ю.Г. Доказывание как вид уголовно-процессуальной деятельности в уголовном судопроизводстве // Военное право. 2018. №1 (47). С. 222-229.
7. Володина Л.М. Предмет познания и предмет доказывания по уголовному делу // Библиотека криминалиста. Науч. журнал. 2012. № 3 (4). С 184-189.
8. Архив Мирового судьи судебного участка № 2 Тахтамукайского района Республики Адыгея. Дело № 1-7/2017.
9. Мировой суд судебного участка №66 Октябрьского судебного района г.Кирова. Дело № 66/1-7/2017.
10. Баринов С.В. Обстоятельства, подлежащие установлению по делам о преступных нарушениях неприкосновенности частной жизни // Российский следователь. 2016. №10. - С. 7 - 10.
11. Архив Центрального районного суда г. Тулы. Дело № 1-97/2015.
12. Архив Сызранского городского суда Самарской области. Дело №10-8/2017.
13. Баринов С.В. Криминалистическая характеристика личности преступника, совершающего преступные нарушения неприкосновенности частной жизни в киберпространстве // Сибирские уголовно-процессуальные и криминалистические чтения. 2015. №2 (8). С. 111 - 117.

Е.В. Богословская,
прокурор отдела по надзору за исполнением законов о несовершеннолетних прокуратуры Московской области,
аспирант
Академия Генеральной прокуратуры РФ, г. Москва

ПРАКТИЧЕСКИЕ ВОПРОСЫ РЕАЛИЗАЦИИ ПРАВА НА СУДОПРОИЗВОДСТВО В РАЗУМНЫЙ СРОК ПО ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В современном мире развитие киберпреступности и увеличение числа преступлений, совершаемых с использованием информационных технологий стремительно растет. Очевидно, что это связано с развитием экономики, появлением виртуальной валюты

(криптовалюты) и новых цифровых технологий, активным внедрением технологических новшеств во всех сферах человеческой деятельности.

Несмотря на принимаемые правоохранительными органами меры Генеральной прокуратурой Российской Федерации отмечается, что в структуре преступности в последнее время достаточно интенсивно увеличивается удельный вес деяний, совершенных в сферах информационно-телекоммуникационных технологий и компьютерной информации. Так, с 2015 по 2017 год число таких преступлений возросло более чем вдвое – с 43,8 до 90,6 тысяч.

В первом полугодии 2018 года в России зарегистрировано почти 993 тысяч преступлений, из которых 80,1 тысяч, что составляет 8% от общего количества, совершены с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации. Наиболее популярными способами совершения таких деяний являлись случаи с использованием сети «Интернет» (49 794), средств мобильной связи (27 026), компьютерной техники (7 718).

В законодательстве критерии отнесения преступлений к киберпреступности и как таковое ее понятие отсутствуют. Ученые предлагают следующие определения. Так, В.А. Номоконов и Т.Л. Тропина киберпреступностью называют совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, сетей и данных [1, с. 45 - 52]. С.В. Скляров и К.В. Евдокимов рассматривают компьютерную преступность в широком смысле по объему и содержанию шире таких понятий, как киберпреступность, интернет-преступность, преступность в сфере компьютерной информации и преступность в сфере информационных технологий [2, с. 322 - 330].

Полагаем, что понятие киберпреступности в целях установления единого подхода к такого рода преступлениям и создания эффективной системы уголовно-правового противодействия должно максимально широко охватывать различные виды преступлений, совершаемые в информационной среде, причем с использованием всевозможных технических устройств.

Полученные статистические данные анализируемой группы преступлений позволяют судить о незначительной эффективности действующих уголовно-правовых норм, высокой степени латентности данной группы преступлений и о необходимости принятия кардинальных мер. Проводимые реформы правового регулирования в данной сфере должны учитывать стремительную динамику процессов

цифровизации криминальных деяний. Следует признать, что стагнация правовых норм не позволяет своевременно реагировать на возникающие проблемы, связанные с предотвращением, раскрытием и расследованием киберпреступлений. Это наблюдается не только в уголовном праве и криминалистике, но и в уголовном процессе.

Преступления, совершаемые в сфере информационно-телекоммуникационных технологий отличаются сложностью выявления, низкой эффективностью раскрытия и судебного рассмотрения [3].

Учитывая отмеченные обстоятельства нельзя недооценивать роль прокурорского надзора за расследованием преступлений в сфере информационно-телекоммуникационных технологий. Своевременное выявление нарушений уголовно-процессуального законодательства, применение мер прокурорского реагирования способствуют достижению целей правосудия, наказанию виновных лиц и осуществлению уголовного судопроизводства в разумный срок.

Прокурору необходимо уделять пристальное внимание соблюдению законности и разумных сроков уголовного судопроизводства о преступлениях в сфере компьютерной информации на стадии возбуждения уголовного дела. Не даром существует мнение, что на практике свыше 90% преступлений в сфере компьютерной информации являются латентными (скрытыми) [4].

Особое внимание следует обратить на способы совершения таких преступлений, которые не всегда являются очевидными, принимая во внимание технический прогресс и личности преступников, обладающих специальными познаниями в области компьютерных технологий.

При решении вопроса о возбуждении уголовного дела прокурор должен тщательно изучить материалы проведенной доследственной проверки, установить наличие сведений о нарушении конфиденциальности информации, правомерность выполненных действий по доступу к компьютерной информации, персональным данным и прочее, размер причиненного ущерба в результате преступных действий злоумышленника, проверить наличие причинно-следственной связи между наступившими негативными последствиями и действиями злоумышленника.

Несвоевременное выполнение неотложных следственных действий ведет к утрате вещественных доказательств, назначению дополнительных судебных экспертиз, что негативным образом сказывается на сроках предварительного расследования. Задачей прокурора в целях предотвращения нарушения прав граждан на доступ

к правосудию и сокращения времени рассмотрения сообщения о преступления, соблюдения требований ст. 61 УПК РФ является своевременное выявление нарушений, особенно в стадии возбуждения уголовных дел по преступлениям, совершаемым с применением информационных технологий.

На стадии возбуждения уголовного дела необходимость в неукоснительном осуществлении прокурорского надзора объясняется бесчисленными нарушениями уголовно-процессуального закона, допускаемыми при разрешении сообщения о преступлении. Такие нарушения могут выражаться в форме:

- отказа в регистрации сообщения о преступлении;
- фальсификацией материалов процессуальной проверки;
- сокрытия от учета преступлений;
- принятия заведомо незаконного процессуального решения об отказе в возбуждении уголовного дела, направлении материала проверки по подследственности в другой орган следствия либо дознания либо иное территориальное подразделение:
- списание материала в номенклатурное дело;
- возбуждение дела об административном правонарушении при наличии признаков состава преступления.

В приказах Генерального прокурора Российской Федерации от 26.01.2017 № 33 «Об организации прокурорского надзора за процессуальной деятельностью органов дознания», от 28.12.2016 № 826 «Об организации прокурорского надзора за процессуальной деятельностью органов предварительного следствия», от 12.07.2010 № 276 «Об организации прокурорского надзора за исполнением требований закона о соблюдении разумного срока на досудебных стадиях уголовного судопроизводства», где акцентируется внимание на необходимости соблюдение процессуальных сроков проведения доследственных проверок, законность и обоснованность их продления, пресечения фактов немотивированной пересылки заявлений и сообщений о преступлениях, материалов проверок и уголовных дел из одного органа предварительного расследования в другой в целях обеспечения прав граждан на судопроизводство и исполнение судебных актов в разумные сроки.

Одним из способов укрытия от учета подобного рода преступлений применяется списание сообщения о преступления сотрудниками органов внутренних дел в номенклатурное дело. В соответствии с п.п. 65, 66 Приказа МВД России от 29.08.2014 №736 «Об утверждении Инструкции о порядке приема, регистрации и разрешения в территориальных органах Министерства внутренних дел

Российской Федерации заявлений и сообщений о преступлениях, об административных правонарушениях, о происшествиях» заявления (сообщения) о происшествиях, когда данные, указывающие на признаки преступления, событие административного правонарушения, не обнаружены, приобщаются к номенклатурному делу, прилагаемому к книге учета сообщений о преступлениях.

По смыслу закона речь идет исключительно о таких заявлениях, в которых не содержится сообщений о преступлении, при этом нередко проверка по ним вообще не проводится. В качестве примера можно привести факты списания сообщений о мошеннических действиях лиц, представлявшихся сотрудниками правоохранительных органов и требовавших по телефону перечисления денежных средств от граждан за непривлечение их родственников к уголовной ответственности якобы в связи с совершением ими преступлений, которые были выявлены при проведении прокурорской проверки. При этом сотрудники внутренних дел, проверяющие такие сообщения, считают, что ущерб никому не нанесен, так как заявителями разгадан замысел неизвестных лиц и не выполнены их требования. Тогда как действия неустановленных лиц должны расцениваться как покушение на мошенничество, т.е. являются преступлением, которое злоумышленники как раз собирались совершить с использованием информационно-телекоммуникационных технологий [5].

Низкой раскрываемости преступлений, совершаемых с использованием информационно-телекоммуникационных технологий способствуют также неудовлетворительное качество проводимых оперативно-розыскных мероприятий и доследственных процессуальных проверок, несвоевременное выполнение неотложных следственных действий, которые приводят к утрате вещественных доказательств, затрате времени на поиски очевидцев, назначению дополнительных судебных экспертиз, что негативным образом сказывается на сроках предварительного расследования. Задачей прокурора является своевременное выявление таких нарушений, в целях предотвращения нарушения прав граждан на доступ к правосудию и сокращения времени рассмотрения сообщения о преступления, соблюдения требований ст. 6.1 УПК РФ.

Список литературы

1. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1 (24). С. 45 - 52.

2. Скляров С.В., Евдокимов К.Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. Т. 10. № 2. С. 322 - 330.

3. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, утвержденные Генеральной прокуратурой Российской Федерации // http://genproc.gov.ru по состоянию на 15.04.2014 (дата обращения 07.12.2018).

4. Линников А.С. Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. 2017. № 5. С. 19 - 29.

5.http://www.kolyma.ru/index.php?newsid=34178http://www.kolyma.ru/index.php?newsid=34178 (дата обращения 07.12.2018). http://www.yuga.ru/news/295667/ (дата обращения 07.12.2018).

М.А. Болвачев,
аспирант
Юридический институт Балтийского федерального университета имени им. И.Канта, г. Калининград

К ВОПРОСУ О ПОНЯТИИ МЕСТА СОВЕРШЕНИЯ ПРЕСТУПЛЕНИЯ В ПРОСТРАНСТВЕ СОЦИАЛЬНЫХ СЕТЕЙ

Повсеместное использование компьютерных технологий, характеризующееся как качественным, так и количественным ростом, широкая доступность компьютерной техники, существенное удешевление доступа к сети Интернет оказывают существенное влияние на развитие глобальной сети, что позволяет говорить о сформированном виртуальном пространстве взаимодействия людей.

Децентрализованный характер и отсутствие контроля за пространством сети Интернет предоставляет новые возможности для преступной деятельности, вследствие чего происходит активное использование сети Интернет в преступных целях. Кроме того, преступная деятельность не ограничивается исключительно компьютерными преступлениями, перечисленными в главе 28 УК РФ, использование сети Интернет возможно и при совершении более

«традиционных» преступлений, таких как мошенничество, клевета, оборот порнографических материалов, склонение к употреблению наркотических веществ, вымогательство и т.п. Необходимо отметить факт заметной переориентации на использование Интернет-технологий при совершении различных преступлений организованных преступных формирований не только транснационального но и вплоть до регионального характера. Вместе с тем, особое место среди наиболее посещаемых интернет-ресурсов занимают социальные сети. Так, около 85% всех пользователей сети Интернет состоят хотя бы в одной социальной сети [1], что привело к активной преступной деятельности в них.

Отмечается, что осмотр места происшествия является одним из важнейших и первоначальных следственных действий, с которого, как правило начинается весь ход расследования преступления. Однако если объективная сторона преступления реализуется в виртуальном пространстве достаточно сложно определить фактическое место совершения преступления. К числу таких преступлений можно отнести[2]:

- Общественно опасные деяния, связанные с незаконным оборотом наркотических средств и психотропных веществ;
- Интернет-мошенничество;
- Вымогательство;
- Преступления, связанные с экстремистской и террористической деятельностью:
- Преступления, связанные с незаконным распространением порнографических материалов;
- Нарушение неприкосновенности частной жизни и тайны переписки;
- Преступления против свободы, чести и достоинства личности;

Возникает проблема определения места совершения преступления, под которым традиционно понимается описанная в законе конкретная территория, на которой совершается преступление. Такой подход в полной мере соответствует пониманию места как части пространства. Социальная сеть, будучи интернет страницей, расположенной на одном из серверов, представляющей собой компьютерную информацию – совокупность электрических сигналов, не является и не может являться частью пространства.

При таком подходе, можно выделить следующие возможные варианты места совершения преступления:

- Место нахождения злоумышленника,
- Место нахождения потерпевшего

- Местоположение сервера, на котором хранятся данные социальной сети.

Наиболее предпочтительным и логичным, на первый взгляд, представляется определение места совершения преступления по месту, где физически находится социальная сеть – сервер. Однако в связи с масштабами современных социальных сетей представляется невозможной непосредственная работа с сервером и его поиск. Так, количество серверов социальной сети «ВКонтакте» превышает десять тысяч. Кроме того, поиск серверов не имеет практического значения, поскольку совершение преступления в пространстве социальной сети образует следовую картину, состоящую из цифровых следов, для изучения которых отсутствует необходимость в непосредственной работе с сервером. Разумеется, не будет по местоположению сервера и других следов, поскольку ни злоумышленник, ни потерпевший там находиться не могли.

Местоположение потерпевшего от вымогательства в социальной сети, мошенничества или иного преступного деяния на момент совершения преступления может содержать информацию о преступном результате или следы реализации объективной стороны преступления. Однако поскольку взаимодействие людей в социальной сети происходит опосредовано, через аккаунты, доступ к которым может осуществляться независимо от устройства (информация храниться на серверах социальной сети), местоположение потерпевшего на момент совершения преступления не содержит никакой информации о преступлении, которая не может быть получена удаленно. Немаловажно отметить, что существенной особенностью, к примеру, преступлений экстремистской направленности в пространстве социальных сетей является проблема определения личности потерпевшего. При совершении преступления в пространстве социальной сети экстремистские материалы, как правило, носят обезличенный характер, направленный не на конкретного человека, но на расу, этнос, национальной или конфессию. Что в принципе исключает возможность определения конкретного потерпевшего.

В ходе взаимодействия злоумышленника с компьютерной техникой образуются как материальные следы физического контакта, так и цифровые следы действий внутри системы используемого устройства. Однако находясь за компьютерным устройством, злоумышленник совершает действия, следы которых распределяются по множеству объектов, не связанных с его местоположением. Такими объектами являются его страница в социальной сети, страница группы

или другого лица, где реализовывалась объективная сторона преступления, промежуточные узлы, система провайдера Интернет-соединения [3]. Вместе с тем, важно отметить, что многие современные компьютерные устройства характеризуются портативностью, к числу таких устройств, с помощью которых возможно осуществлять выход в Интернет и, соответственно, возможно совершить преступление относятся и смартфоны. В таком случае, преступление может быть совершено из любой точки, плоть до общественного транспорта. Лицо, использующее компьютерное устройство для совершения преступления может как находиться в видимости третьих лиц, так и нет, тем не менее, внешняя неотличимость преступных и непреступных действий без наблюдения за экраном устройства нивелирует целесообразность обозначения таких лиц в качестве очевидцев. Кроме того, на момент начала расследования, когда осмотр места происшествия критически важен, отсутствует какая-либо информация за исключением, находящейся в социальной сети, в следствии чего, осмотр места нахождения злоумышленника не представляется возможным.

В таком случае, ни одна из представленных альтернатив не имеет практической пользы.

Вместе с тем, важно заметить, что в пространстве социальных сетей в основном пребывают подростки и молодежь, являющиеся наиболее мобильной и уязвимой частью населения. Интернет-пространство создает принципиально отличную от реального мира среду, характеризующуюся высокой степенью доверия к информации и собеседникам, действующим в сети Интернет [4]. В следствии чего, Интернет-пространство человеком на подсознательном уровне не воспринимается как источник опасности, что позволяет злоумышленнику широкие возможности для подготовки и совершения преступлений и где остается подавляющая часть информации о преступлении.

Проведение следственных действий и оперативно-розыскных мероприятий в социальной сети неразрывно связано с проблемами их законодательного регулирования. В уголовно-процессуальном законодательстве предусмотрено проведение осмотра места происшествия, местности, жилища, иного помещения, предметов и документов, в следствии чего достаточно сложно определить, чем будет являться осмотр социальной сети как интернет-страницы. Отмечается отсутствие криминалистических рекомендаций по алгоритму фиксации контента в сети Интернет, эталонам оформления материалов, требования к ним, а также программного обеспечения,

которое может быть использовано при проведении следственных действий и оперативно-розыскных мероприятий сети Интернет [5].

Установление места совершения преступления необходимо для точной криминалистической характеристики преступления, поскольку выступает стартовой точкой процесса расследования. В отношении данных преступлений целесообразно расширительно толковать место, включая в него виртуальное пространство социальной сети, где будет находиться интересующая следствие информация в виде переписки, опубликованных материалов, лог-файлов, IP-адресов. Именно там должен начинаться процесс расследования таких преступлений. Вместе с тем, проблема расследования преступлений в пространстве социальных сете сохраняет свою актуальность и требует комплексного подхода к ее дальнейшему исследованию.

Список литературы

1. Воронкин А.С. Социальные сети: эволюция, структура, анализ //"Образовательные технологии и общество". - 2014. - № 9. - 650-675.

2. Соловьев В.С. Преступность в социальных сетях интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. - 2016. - Т. 10, № 1. - С. 61-70.

3. Введенская О.Ю. Особенности следообразования при совершении преступлений посредством сети Интернет // Юридическая наука и правоохранительная практика. - 2015. - № 4. - С. 209-216.

4. Григорьев А.Н., Бодылина Э.А., Информационно-телекоммуникационная сеть Интернет как среда и средство совершения преступлений // Материалы международной научно-практической конференции "Закон и правопорядок в третьем тысячелетии". Калининградский филиал Санкт-Петербургского университета МВД России. -2017. -72-73.

5. Волчецкая Т.С., Загоскин А.В. Современные проблемы профилактики терроризма и экстремизма и пути их решения с позиций ситуационного подхода // Ситуационный подход в решении современных проблем противодействия терроризму и экстремизму: материалы Всероссийской научно-практической конференции «Противодействие терроризму и экстремизму: ситуационный подход (в условиях организации и проведения крупных спортивных мероприятий, с учетом геополитического положения региона)»/Под ред. Т.С. Волчецкой. Калининград. - 2017. - С.6-14.

А.А. Васильев,
д.ю.н., доцент, заведующий кафедрой теории и истории государства и права
Алтайский государственный университет, г. Барнаул

О.В. Васильева,
соискатель кафедры теории и истории государства и права
Алтайский государственный университет, г. Барнаул

Д. Шпопер,
д.ю.н., профессор
Поморская академия, Польша, г. Слупск

«УМНЫЕ МАШИНЫ» И ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ КАК ВЫЗОВЫ ДЛЯ ЭТИКИ И ЮРИСПРУДЕНЦИИ

Научно-техническая революция в XXI в. приобрела новые очертания в сфере цифровых технологий. В сфере программирования одним из достижений стали разработки в сфере искусственного интеллекта и робототехники [1]. При серьезном потенциале в использовании искусственного интеллекта в различных областях жизнедеятельности остаются слабо изученными этические и правовые аспекты использования искусственного интеллекта [2].

Более того, реальное применение искусственного интеллекта практически не обеспечена должной международно-правовой и национальной нормативной основой. Вопросы использования "умных роботов" лишь спорадически регулируются в отдельных государствах мира - Германии, Южной Кореи, Франции. В ЕС принята резолюция "Нормы гражданского права о роботехнике" от 16.02.2017 г. Единственным исключением в России выступает так называемый "закон Гришина" - закон "О роботехнике", разработанный юридической фирмой Dentons [3].

Среди юридических граней использования искусственного интеллекта можно назвать следующие:

Во-первых, отсутствует четкая юридическая дефиниция искусственного интеллекта. Для должного определения можно бы было опереться на понимание искусственного интеллекта в специальных науках.

Во-вторых, возникает вопрос о возможности признания за искусственным интеллектом качеств субъекта права [4]. Здесь

возможно два варианта. В первом случае искусственный интеллект понимается всего лишь как техническое средство с правовым режимом вещи. Во втором случае за ним признается статус электронного лица по аналогии с юридическим лицом через использование приема правовой фикции. И тот и другой случай не в полной мере адекватны. Квалификация искусственного интеллекта как объекта права не учитывает наличие некой субъектности - способности к мышлению и принятию самостоятельных решений. Во втором случае поднимается более глубокий вопрос мировоззренческого порядка - искусственный интеллект - это личность подобная человеку. От решения данного вопроса зависит модель правового регулирования, начиная с возможности вступления в правоотношения и до возложения на такой интеллект юридической ответственности.

Соответственно, третий аспект применения искусственного интеллекта поднимает проблему ответственности за вред, причиненный таким интеллектом. В юридической литературе обсуждаются различные модели возложения деликтной ответственности:

- обладатель прав на устройство, снабженное искусственным интеллектом;
- разработчик программного обеспечения;
- оператор, обслуживающий искусственный интеллект.

Вполне обсуждаемым выглядит возможность применения к искусственному интеллекту конструкции источника повышенности ответственности, при которой за вред причиненный таким объектом возмещения вреда наступает без учета вины собственника объекта.

Следует отметить, что искусственный интеллект ставит вопрос о судьбе самой юридической профессии. Искусственный интеллект вполне способен выполнять типичные юридические действия по заданному алгоритму: составление сделок, исковых заявлений и пр. Крупные компании в России, в том числе Сбербанк, ВТБ планируют широко использовать нейронные сети для такого рода работы. Естественно, в принципе заменить человека искусственный интеллект не может, поскольку не рассчитан на решение нестандартных ситуаций с учетом сугубо человеческих свойств - совесть, справедливость, милосердие и пр. Хотя ведущие разработчики в сфере искусственного интеллекта серьезно заявляют о том, что загруженные базы данных (законодательство, судебная практика, доктринальные источники) для нейронных сетей позволят искусственному интеллекту сформулировать и применить принципы права. Американские исследователи полагают на основе эксперимента по анализу решений

ЕСПЧ искусственным интеллектом, что он способен предсказывать решения судов. В 79 % искусственный интеллект смог предсказать решение ЕСПЧ на основе изучения материалов дела [5].

Этическая проблема отношения к искусственному разуму как личности, равной человеку. Как следствие, вопрос о признании за ним статуса юридической личности. Во многом решение этих вопросов зависит от понимания человеческого интеллекта и его особенностей. Только полное принципиальное тождество человеческого и искусственного интеллекта может привести к признанию за искусственным интеллектом качеств личности как в этическом, так и правовом отношении. Очевидно, что при всем многообразии определений интеллекта и разума, искусственный интеллект не обладает такими качествами как сознание и эмоции, которые определяют человеческую природу.

При этом, возникает предварительный вопрос определения разума, его качеств и соотношения со смежными категориями – машинное обучение, нейронные сети, который не может быть решен иначе как через консенсус представителей различных отраслей знания на основе широкой дискуссии (философия, психология, нейробиология, этика, юриспруденция, кибернетика и т.д.).

Признание личностного статус за искусственным интеллектом с непреложностью приведет к гуманизации отношения к умным машина. Как следствие, такие умные роботы могут быть признаны квазилицами (юридическими лицами) с соответствующими правовыми последствиями - правосубъектность, способность вступления в правоотношения и возникновения деликтной ответственности.

Среди вопросов, которые нуждаются в научном, а впоследствии и нормативном решении выступают:

1. Юридическая дилемма – умный робот есть субъект права с собственной волей или объект правоотношения? [6]
2. Логическим следствием выступает вопрос о возможности робота вступления в правоотношения и возложения на него ответственности за неисполнение обязанностей и причиненный вред. Либо умный робот - это субъект как юридическое лицо с ответственностью (закрепление за ним имущества и страхование ответственности) либо объект (посредник) с возложением ответственности на одно из лиц (программист, продавец, собственник, сервисная служба, страховая компания и т.п.).
3. Еще одним интересным вопросом выступает роль технических и технико-юридических норм в создании и применении искусственного интеллекта [7]. Отказ от признания за умным роботом

прав лица будет означать применение к нему технических и технико-юридических норм. Так, в скорейшей фиксации нуждаются на национальном и международном уровне правил относительно недопустимости причинения роботом вреда человеку. В цифровой код умного робота должен быть включен внутренний ограничитель – «совесть робота», отключающий устройство при угрозе нанесения вреда человека. Требуется разработка стандартов безопасности искусственного интеллекта в сочетании с государственным контролем за их соблюдением. Этот вопрос приобретает особую остроту, поскольку отсутствует полная информация о последствиях применения искусственного интеллекта. До конца неясно возникнет у умного робота самоидентификация или желание приобрести человеческое естество и не сможет ли он стать полностью автономным человека и неуправляемым.

4. Последствия внедрения искусственного интеллекта в юридическую профессию.

Плюсы:

- освобождение юристов от рутинных операций и возможность занятия творческим трудом;
- обработка массивов правовой информации – устранение противоречий и дублирования;
- вспомогательный ресурс для решения юридических дел;
- нейтрализация негативных последствий субъективного фактора в юридической профессии.

Минусы и проблемы:

- угроза потери работы юристами;
- недоверие к умным машинам как судьям и пр.;
- вопрос о возможности с использованием искусственного разума справедливого решения дела и проявлении именно человеческих качеств при разрешении споров (милосердие, добросовестность, справедливость и т.п.).

Следует отметить, что появление цеха юристов во многом связано с необходимостью поиска, истолкования и применения юридических норм в ситуации правовой неопределенности возникшей конфликтной ситуации. Для корпорации юристов всегда были характерны кастовый и закрытый характер. Не случайно, что знание первых законов, ведение судебного календаря и судебных исков было тщательно охраняемой профессиональной тайной первых римских юристов - жрецов-понтификов. И даже публикация первых правовых текстов не привела к ликвидации юридического сословия, поскольку не была снята сама проблема неопределенности содержания норм

права. Значение юристов в тем большей мере возрастало, чем более непонятной, массивной и противоречивой становилась система правовых норм. Совершенно очевидно, что английское прецедентное право имеет выгоды исключительно для массы английских юристов, а не их клиентов, которым гонорары солиситоров и барристеров обходятся весьма недешево.

Полагаем, что применение искусственного интеллекта в сфере правотворчества может минимизировать фактор правовой неопределенности и приведет к трансформации «человеческого права» в машинный алгоритм, вполне допускающий математическую точность и логику. В таком случае и применение права может быть организовано на основе алгоритмов, исключающих усмотрение и произвол. Как следствие, места человеку в такой правовой системе не остается, поскольку все юридически значимые действия будут определяться цифровым кодом, применяемым умными роботами.

Здесь мы сталкиваемся с более важной проблемой, чем будущее право и юридической профессии. Речь идет о таком социальном укладе, при котором поступки человека будут изначально прогнозироваться и корректироваться с точки зрения соответствия некоему эталону – алгоритму при тотальном контроле за поведением человека с помощью умных машин. Такой социальный порядок будет подобен действию технических устройств на основе инструкций. Возможно, в таком технологическом тоталитаризме и не будет места социальным отклонениям, но и человек потеряет свою природу в поиске смысла жизни, поскольку его жизнь будет мелочно и скрупулезно предрешена суперкомпьютером.

Видимо, человечеству в ближайшее время необходимо разрешить для себя эту дилемму – бессмысленный порядок или осмысленный человеческий хаос с возможностью свободы воли; предопределенность или страх перед неизвестным.

Список литературы

1. Келли К. Неизбежно. 12 технологических трендов, которые определяют наше будущее. М., 2017.
2. Росс А. Индустрии будущего. М., 2017.
3. Учеными СПбГУ (В.В. Архипов, В.Б. Наумов) и компанией Dentons (А.Незнамов) создан исследовательский центр проблем правового регулирования искусственного интеллекта и роботехники. // http://robopravo.ru.

4. Архипов В.В., Наумов В.Б. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике // Труды СПИИРАН. 2017. № 6. С. 51.

5. N. Aletras, D. Tsarapatsanis, D. Preoţiuc-Pietro, V. Lampos (2016). Predicting Judicial Decisions of the European Court of Human Rights: A Natural Language Processing Perspective, Peer J Computer Science.

6. Архипов В.В., Наумов В.Б. Искусственный интеллект и автономные устройства в контексте права: о разработке первого в России закона о робототехнике // Труды СПИИРАН. 2017. № 6.

7. Морхат П.М. Искусственный интеллект. Правовой взгляд. М., 2017.

В.Б. Вехов,
доктор юридических наук, профессор, Заслуженный деятель науки и образования РАЕ, профессор кафедры юриспруденции, интеллектуальной собственности и судебной экспертизы Московский государственный технический университет имени Н.Э. Баумана (национальный исследовательский университет), г. Москва

И.М. Комаров,
доктор юридических наук, профессор, профессор кафедры криминалистики Московский государственный университет имени М.В. Ломоносова, г. Москва

ПРЕСТУПЛЕНИЯ В СФЕРЕ ЦИФРОВОЙ ЭКОНОМИКИ: КРИМИНАЛИСТИЧЕСКИ ЗНАЧИМЫЕ СВЕДЕНИЯ О ТЕХНОЛОГИИ «БЛОКЧЕЙН»

В условиях широкого применения информационно-телекоммуникационных и криптографических технологий, стремительного развития электронной торговли и планового перехода на цифровую экономику, создаваемую в соответствии с Распоряжением Правительства Российской Федерации от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации»», преступные посягательства, связанные с

использованием технологии «блокчейн» (от англ. «Blockchain» – «Блоковая цепь»), стали представлять угрозу национальной безопасности. Например, известно, что многие транзакции с использованием криптовалют производятся анонимно, без централизованного контроля со стороны государств и организаторов платежных систем. Это мотивирует преступников к использованию названного средства платежа для совершения преступлений, в том числе таких, как торговля наркотиками, оружием, финансирование терроризма, уклонение от уплаты налогов. Оплата незаконно поставляемых запрещенной в России террористической организацией ИГИЛ нефти и газа, а также вербовка новых членов этой террористической организации осуществлялись с помощью названных электронных платежно-расчетных инструментов [1, с. 128].

Продолжая исследование выделенной проблематики, отметим, что 25 июля 2017 года по запросу американских правоохранительных органов в Греции был задержан российский программист Александр Винник. Прокуратурой города Сан-Франциско (штат Калифорния) ему заочно было предъявлено обвинение в отмывании 4 млрд. долл. США, полученных преступным путем через биржу криптовалют и фиатных денег BTC-e, а также в совершении кибермошенничеств, похищении персональных данных, взломе японской биржи Mt.Gox, спровоцировавший её банкротство, и участие в торговле наркотиками. Примечателен также тот факт, что 10 августа 2017 года названному лицу в Российской Федерации было предъявлено обвинение в мошенничестве в крупном размере: он обманным путем с использованием сети Интернет под предлогом поставки оборудования похитил более 600 тыс. рублей у одной из организаций. А. Винник был объявлен в международный розыск. Останкинский суд Москвы 11 августа 2017 года заочно избрал ему меру пресечения в виде заключения под стражу. Генеральной прокуратурой Российской Федерации в Министерство юстиции, прозрачности и прав человека Греческой Республики было направлено три соответствующих запроса (18.08.2017, 25.12.2017 и 06.07.2018) о его выдаче для привлечения к уголовной ответственности [2, с. 8], последнее из которых 30 июля 2018 года было удовлетворено [3].

Следует признать, что особенности механизма совершения рассматриваемых преступных посягательств, специфичность следовых картин, отличающихся высокой динамикой развития и изменения, изучены явно недостаточно. В связи с чем, считаем целесообразным подробнее остановиться на исследовании криминалистически значимых сведений о технологии «блокчейн».

Виртуальные деньги – это всего лишь один из немногих достаточно широко известных вариантов использования указанной технологии. В проекте Федерального закона № 419059-7 (от 22.05.2018 № 4030-7 ГД), подготовленного ко второму чтению, они названы «цифровым финансовым активом» и определены как «имущество в электронной форме, созданное с использованием шифровальных (криптографических) средств». Право собственности на него удостоверяется путем внесения цифровых записей в реестр цифровых транзакций. К цифровым финансовым активам относятся криптовалюта и токен. Вместе с этим, проект Федерального закона № 424632-7 «О внесении изменений в части первую, вторую и четвертую Гражданского кодекса Российской Федерации» (от 22.05.2018 № 4032-7 ГД) определяет их как «цифровые деньги – совокупность электронных данных (цифровой код или обозначение), созданная в информационной системе, отвечающей установленным законом признакам децентрализованной информационной системы, и используемая пользователями этой системы для осуществления платежей». Из этого следует, что как предмет и средство преступного посягательства криптовалюта, токены или цифровые деньги – это разновидность компьютерной информации, т.е. сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи (прим. 1 к ст. 272 УК РФ). Иными словами, это электронные записи – электронные условные числовые единицы, которые используются участниками соответствующих платежных систем для взаимных расчетов. Данное обстоятельство необходимо учитывать при квалификации преступных деяний рассматриваемой категории.

В отличии от электронных денежных средств, оборот которых регулируется Федеральным законом «О национальной платежной системе» (от 27.06.2011 № 161-ФЗ), они не обеспечены ликвидными активами и какими-либо гарантиями государственного либо частного капитала, в том числе владельцев – организаторов криптовалютных платежных систем, которые не несут перед пользователями никаких обязательств, кроме обеспечения функционирования соответствующих информационных систем, основанных на использовании криптографической технологии распределенных реестров.

В соответствии с п. 3 ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (далее – Закон об информации) криптовалютная платежная система – это информационная система, т.е. совокупность

содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Распределенный реестр есть ни что иное, как распределенная база данных, т.е. представленная в объективной форме совокупность самостоятельных материалов (статей, расчетов, нормативных актов, судебных решений и иных подобных материалов), систематизированных таким образом, чтобы эти материалы могли быть найдены и обработаны с помощью ЭВМ (абз. 2 п. 2 ст. 1260 ГК РФ).

Управление рассматриваемой платежной системой осуществляется ее оператором с помощью специализированного сайта в сети Интернет – совокупности программ для ЭВМ и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети Интернет по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети Интернет (п. 13 ст. 2 Закона об информации).

Фактически, это систематизированная база цифровых транзакций, которые хранятся, одновременно создаются и обновляются на всех электронных носителях у всех участников информационной системы на основе заданных алгоритмов криптографического преобразования данных.

Заметим, что активное обсуждение в мире данной технологии связано с её очевидными экономическими и политическими преимуществами.

Технология «Block Chain» в настоящее время проходит практическую проверку в так называемой «технологической песочнице» – в качестве платежного инструмента в финансовой сфере. Проводятся также эксперименты по возможностям ее внедрения в избирательные процессы, обслуживания земельных кадастров, медицинских, правовых, логистических и других профильных баз данных, где всегда нужна прозрачность, защищенность и безопасность.

Использование технологии «Блокчейн» исключает необходимость привлечения «третьей стороны» при совершении экономических операций, так как система прозрачна для всех. Это свойство делает её защищенной и безопасной для действий сторон в условиях риска мошеннических действий и необходимости сохранения информации. Попытаемся объяснить простыми понятиями. Технология «Block Chain» схожа с технологией «Bit Torrent». На основе последней в сети происходит большая часть обмена контентом.

Такая ее популярность обусловлена наличием ряда достоинств. Во-первых, отсутствует центральный сервер, то есть вся база данных распределена среди участников-пользователей, а это обстоятельство указывает на невозможность несанкционированного проникновения в систему посторонних лиц; во-вторых, у каждого пользователя имеется полная копия базы (содержащая всю цепочку транзакций) в зашифрованном виде; копии синхронизируются с целью достижения консенсуса (это алгоритм решения по конфликтующим версиям блокчейна); в третьих, любой пользователь в состоянии отследить любую транзакцию (система полностью прозрачна); в четвертых, информация в базе построенной по технологии блокчейн добавляется в виде новых блоков и это добавление согласуется с другими пользователями сети (на примере «биткойна», новая единица этой криптовалюты добывается путем ресурсоемких расчетов, перебора чисел и расчета для них хеша с целью вписаться в заранее заданный шаблон). Добытую новую единицу «биткойна» (по существу – новый блок информации) проверяют другие участники системы, на основе пересчета хеш суммы и только после этого данный новый блок вписывается во все базы всех пользователей системы.

Повторимся, система устроена так, что все незаконные попытки внесения изменений в базу, которая основана на технологии блокчейн («похитить» блоки, то есть приписать их себе или добавить новые блоки) всегда пресекаются пользователями посредствам сравнения с копиями хранимых у них баз. Взломать систему также практически невозможно по двум причинам: её децентрализации и многократного копирования хранимой пользователями информации. Это можно сравнить с организацией ДНК в клетках человека. Их много, и они несут в себе всю полноту информации, а при возникновении сбоев легко справляются с ними в отдельных копиях.

Можно привести и другой ассоциативный ряд иллюстрирующий, что такое технология «Block Chain». Представим себе облачное хранилище, доступное всем в полном объеме, где находится большое количество папок с файлами. Там любой пользователь может видеть, что в данный момент «залито», где находятся определенные файлы и кто с ними работал («заливал», «качал»). Однако обладая этой информацией любой пользователь может скачивать только то, на что он имеет право, также и «заливать» файлы в систему он может только после того как выполнит условия, оговоренные указанной системой.

Теперь пример работы рассматриваемой технологии рассмотрим в аспекте цифровых денег. В данных платежных системах

нет персональных «кошельков» – «личных кабинетов», т.е. отсутствуют данные, доступные только владельцу «кошелька» – участника системы. Имеется один «кошелек», однако вся информация о нем открыта для всех участников системы, что означает – статистика всех межличностных расчетов прозрачна. Вмешаться в расчеты двух участников системы (изменить порядок и характер расчетов, совершить хищение и т.п.) третий её участник не может ни при каких обстоятельствах, по причине того, что так система логически устроена. Участник системы, между тем, всегда может получить только ему одному предназначенный расчет, он «привязан» к определенным адресам, между которыми и осуществляется транзакция. Получение расчета подтверждается (подписывается) ключом совместимым с адресом (по существу это логин и пароль), а данные о проведении расчета пересылаются по всем копиям базы. Транзакция считается завершенной по окончании сверки записи об отправке и получении расчета.

Что из себя представляет криптовалюта? По идее разработчиков – это «золото» виртуального мира. Количество этого «золота» ограничено расчетами возможного предельно допустимого числа его наличия в каждой конкретной системе. Предлагаются три пути добычи цифровых денег:

1) приобретение в виртуальном пункте обмена валюты;

2) на виртуальной бирже;

3) путем непосредственной «добычи» – «майнинга», т.е. деятельности, направленной на создание криптовалюты и/или валидацию с целью получения вознаграждения в виде криптовалюты.

Эти операции доступны любому пользователю информационно-телекоммуникационной сети Интернет, при условии наличия у них соответствующего программно-технического оборудования.

Вместе с тем, использование технологии исследуемого вида сталкиваются с рядом проблем. Так, для поддержания высокого уровня безопасности система постоянно нуждается в сложных вычислениях, что возможно только на основе высокой ресурсной базы. Для биткойнов разработчики эту проблему решили просто. Пользователям, которые связаны с «добычей» «биткойнов» назначают комиссию с тем, чтобы они предоставили свой ресурс, то есть подтвердили возможность майнинга (способ заработка биткойна).

Кроме того, для безопасности системы важно, чтобы ресурсная база была распределена, а не находилась под управлением группы, которая может использовать ресурсы для различных манипуляций.

Как было изложено ранее, криптовалюта не обеспечена никакими экономическими факторами (золото, уровень ВВП и т.д.), поэтому её курс может легко обваливаться до полного нуля. Этот и другие экономические недостатки вызывают к ней недоверие правительств многих государств. Так, о необходимости запрета подобного рода платежных средств указано и в рекомендациях, подготовленных по итогам экстренной встречи министров юстиции стран ЕС, прошедшей в ноябре 2015 года в Брюсселе (встреча прошла после терактов во Франции) [4]. Однако в отдельных государствах имеются экономические учреждения, интернет-магазины или сервисы, которые принимают «биткойны» в качестве оплаты за товары и услуги.

В современном мире виртуальную валюту можно обменять на рубли, доллары, электронные деньги с помощью онлайн-серверов, таких как, например, 60сек, BaksMan, Ychanger, 24PayBank, ProstoCash, WMGlobus, Xchange. Известны также криптобиржи EXMO, BitFlip, BitMEX, LocalBitcoins и др.

Продолжая исследование выделенной проблематики, отметим, что в настоящее время в обороте находится около 600 различных криптовалют [5]. Вместе с этим, чаще всего платежные операции совершаются в «биткоинах» (54,3%), «эфириумах» (20,3%), а также в «риппле» (4,5%) [6].

В мировом рейтинге по числу пользователей этими расчетными средствами Россия занимает пятое место. Тройку лидеров формируют США, Китай и Германия [7].

В качестве выводов можно отразить преимущества и недостатки криптовалюты в отношении реально существующих валют.

Привлекательным является независимость системы, её абсолютная защищенность от различных внешних воздействий. При этом прозрачность отношений с криптовалютой доступна каждому пользователю, но влиять на эти отношения он никак не может. Видимо, поэтому в 2016 году Международная организация по стандартизации (ISO) создала специальный комитет для разработки стандарта технологии Блокчейн. В него вошли и четыре представителя от Российской Федерации – члены комитета по разработке стандартов в области криптографической защиты информации Федерального агентства по техническому регулированию и метрологии. Их задача состоит в том, чтобы в международный стандарт названной технологии вошли российские криптографические алгоритмы защиты информации. В настоящее время во всех технологиях Блокчейна

используются зарубежные средства электронной подписи, что сдерживает их широкое распространение в России [8].

Наличный объем «биткойнов» всегда ограничен, тиражировать (напечатать) по чьему-то желанию эту валюту невозможно. Её «добыча» сложна с позиции технического подхода. Известны расчеты, которые свидетельствуют, что жизнеспособность криптовалюты обеспечена определенным алгоритмом и «добыть» возможно не более 21 млн. «биткойнов». После этого «добыча» не возможна. Сейчас нельзя прогнозировать последствия этого факта, но можно с уверенностью сказать, что при всех благоприятных обстоятельствах криптовалюта останется в обращении с периодическим изменением курса.

Между тем недостаточная популярность криптовалюты может быть ещё и существенным плюсом для неё, ибо изначально распределительная модель блокчейна несет в себе и некоторые ограничения, в том числе и по числу проводимых транзакций и объему хранимой базы данных. По этой причине в августе 2017 года от основной ветки криптовалюты был отделен «биткойн хеш», так как увеличение числа участников привело к замедлению прохождения платежей в системе.

Тема технологии «Block Chain» и криптовалют, на наш взгляд, находится ещё в начале пути, ей нет ещё и десяти лет, между тем криминалистика должна располагать основами соответствующих знаний для того, чтобы быть готовой в нужный момент «вмешаться» в определенные процессы, где могут усматриваться нарушения действующего законодательства и потребуется установить следы нарушений для принятия решения о возможном криминальном характере события.

Подобные проблемы уже возникают в связи с не персонифицированным характером майнинга получения криптовалюты. Этот достаточно широкий круг субъектов как физических, так и юридических лиц фактически получают средства для совершения различных финансовых операций и при определенных обстоятельствах могут быть вовлечены в противоправную деятельность различной направленности (легализация доходов, полученных преступным путем, финансирование терроризма и экстремистской деятельности и т.п.). Криптовалюты могут быть использованы в качестве расчетного средства за результаты противоправной деятельности.

Можно и далее приводить абстрактные примеры тактических криминалистических возможностей доказывания использования

преступниками криптовалюты в качестве средства платежа за различные криминальные услуги. Однако, это мало повлияет на уже вероятно формирующуюся криминальную ситуацию, где указанные валюты планируются как средства соответствующего платежа. Полагаем, что криминалистам необходимо обратиться к этим вопросам уже «вчера» и на основе данных криминалистической тактики с участием соответствующих профильных специалистов разрабатывать и совершенствовать необходимые рекомендации следственной деятельности.

Список литературы

1. Вехов В.Б. Особенности расследования преступлений, связанных с оборотом виртуальных денег // Расследование преступлений: проблемы и пути их решения. 2016. № 3. С. 127-130.

2. Бычков В.В., Вехов В.Б. Специальные знания, обеспечивающие расследование преступлений, связанных с оборотом криптовалюты // Российский следователь, 2018. № 2. С. 8-11.

3. Суд в Греции удовлетворил запрос Генпрокуратуры России об экстрадиции Винника. URL: https://russian.rt.com/world/news/540928-sud-greciya-ekstradiciya-vinnik.

4. Козлова Н. Обман валют. URL: http://rg.ru/2016/01/15/bastrykin.html.

5. Япония признала криптовалюты законным платежным средством. URL: https://news.mail.ru/economics.

6. Смирнова Е., Мухаметшина Е. ФСБ участвует в разработке международного стандарта блокчейн. https://www.vedomosti.ru/technology/articles/2017/08/18/730045-fsb-blokcheina.

7. Маркелов Р. Биткоинам объявили войну. URL: http://rg.ru/2016/02/29.

8. Смирнова Е., Мухаметшина Е. ФСБ участвует в разработке международного стандарта блокчейн. https://www.vedomosti.ru/technology/articles/2017/08/18/730045-fsb-blokcheina.

Е.С. Витовская,
преподаватель кафедры уголовного права
Кузбасский институт ФСИН России, г. Новокузнецк

К ВОПРОСУ О ПРОТИВОДЕЙСТВИИ ПРЕСТУПЛЕНИЯМ НАРКОТИЧЕСКОЙ НАПРАВЛЕННОСТИ, СВЯЗАННЫМ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ СРЕДСТВ

Незаконный оборот наркотических средств и психотропных веществ является сложным преступлением, поскольку его общественная опасность раскрывается не только через общественные отношения, охраняющие здоровье населения, но и через широкий круг иных общественных отношений. Наркотизм представляет проблему глобального уровня, поскольку подрывает здоровье и генофонд нации, безопасность, экономику, социальную сферу, деятельность государственных ведомств, нравственную основу общества, внешнеэкономические связи между государствами. Затраты на противодействие незаконному наркообороту огромны, систематически укрепляются силовые структуры и судебная система; разрабатываются и апробируются комплексы наркологической помощи наркозависимым; высоки расходы на здравоохранение и социальную сферу.

Правовое регулирование противодействия незаконному обороту наркотиков опирается также на нормы международного права. Очевидно, что незаконный наркооборот наносит, если не прямо, то опосредованно, ущерб отношениям международного сотрудничества. По данным ООН, в 2017 году международными правоохранительными ведомствами выявлено 5 тыс. международных преступных групп, деятельность которых так или иначе была связана с незаконным оборотом наркотиков. В 2014 году транснациональные организованные преступные группы от незаконного наркооборота получили приблизительно от пятой до третьей части своей прибыли [1, 11]. В июле 2015 года выступая на международной конференции «Московско-Африканский антинаркотический диалог» в Гамбии В.П. Иванов отметил, что наркотики являются аналогом золотовалютных резервов для лжегосударственных формирований «Исламское государство» и «Боко Харам», их доходы от незаконного наркооборота составляют 500 млрд. долл. США[2].

Имеется множество свидетельств того, что наибольший процент наркооборота приходится на анонимную сеть, поскольку появление

маршрутизаторов, подключенных к сети Интернет, усовершенствование возможностей мобильной связи открыли перед наркодилерами новые возможности совершать с использованием компьютерных средств преступления наркотической направленности. Так, отсутствует необходимость в личном контакте сбытчика и приобретателя наркотиков. Сбытчик создает интернет-сайт с целью торговли наркотиками, приобретатели наркотиков с использованием криптовалюты обеспечивают анонимный платеж. После получения платежа наркосбытчик скрытым образом делает «закладку» и сообщает своим клиентам о месте, где можно забрать наркотики, через сообщения с использованием средств шифрования, встроенных в различные виды устройств. Использование новых информационно-коммуникационных технологий в организации и функционировании нелегального наркооборота ведет к увеличению объемов сбыта наркотиков. В криминальной деятельности используются высокие технологии, характеризующиеся анонимностью сведений о владельце ресурса; отсутствием требований идентификации или подтверждения; защитой информации шифром или цифровым форматом (TrueCrypt, BitLocker); ограничением доступа к личным архивам; хранением информации на удаленных серверах; использованием приложений, временно хранящих информацию (Snapchat, Wickr), криптоустойчивых мессенджеров и анонимных систем виртуальных туннелей, применяющих специальные веб-браузеры и уникальные домены (Tor, DarkNet, Telegram,Jabber,RetroShare, I2P, P2P, FreeNet, Riffle); использованием торговых площадок в «темной сети» (AlphaBay, Cryptomarket, Hansa, Nucleus). Кроме того, по-прежнему, используются одноразовые сотовые устройства, ресурсы интернет-кафеи SIM-карты, не требующие регистрации, зарегистрированные на иных лиц, либо копии чужих SIM-карт.

Все чаще в различных источниках употребляются термины «банкинг», «блокэксплорер», «блокчейн», «майнинг», «криптовалютная биржа», «криптовалюта», «биткоин», «эфир», «альткоин», «лайткоин», «токен», «бэкдор», что свидетельствует о появлении новыхкрипто-технологий, которые не только развивают электронные платежные системы, но и позволяют избежать риска изобличения преступным наркогруппам. Так, в 2016 году четверть выручки крипторынки получили от опосредованного участия в незаконном наркообороте, при этом значительная часть выручки поступала от сделок на сумму от 100 до 1 000 долл. США [3, 31].

Исследование сложного механизма воздействия государства на наркотизм немыслимо без оценки такой криминологической

категории, как противодействие. Проблеме противодействия преступлениям в сфере незаконного оборота наркотических средств и психотропных веществ, связанным с использованием компьютерных средств уделено большое внимание. Так, Литва является инициатором создания киберсил быстрого реагирования. В рамках данного проекта запланирован обмен информацией, достижениями и опытом специалистов. Международное сотрудничество предполагает создание инструментов киберзащиты, проведение совместных тренировочных учений и применение механизмов привлечения к ответственности за правонарушения в киберпространстве [4]. Необходимость противодействия нелегальному наркообороту с использованием компьютерных средств определена Конгрессами ООН по предупреждению преступности и уголовному правосудию. В апреле 2015 г. в Дохе состоялся Конгресс ОНН, в котором приняла участие делегация Российской Федерации [5]. В резолюции, принятой Конгрессом, говорится о взаимном сотрудничестве, реализации совместных программ, эффективном обмене информацией, сведениями и опытом об эффективных механизмах противодействия преступным связям транснациональной организованной преступности, участвующей в незаконном наркообороте при использовании современных информационно-коммуникационных технологий. Кроме того, предлагается реализовывать меры, направленные на создание защищенной киберсреды и противодействие криминальной деятельности, осуществляемой с помощью сети Интернет. В ходе Конгресса проведен семинар-практикум, посвященный информационной преступности, на котором дифференцированы киберпреступления: правонарушения, направленные против свойств компьютерных систем; правонарушения, связанные с использованием компьютерных средств; правонарушения, связанные с содержанием компьютерных данных. Участники дискуссии пришли к мнению, что киберпреступность относится к сложному и многогранному явлению, с новым modioperandi, используемым для совершения рассматриваемых преступлений. Проанализированы вопросы использования геолокации и WHOIS, а также проблемы в способах измерения, отслеживания и сбора данных. Отмечено, что существует возможность сохранения контента после произведенного ареста и закрытия сервера. Акцентировалось внимание на том, что большое количество вопросов возникает при оценке цифровых доказательств, это представляет сложность в деятельности правоохранительных ведомств. В обеспечение деятельности силовых структур предложено привлекать внешних подрядчиков либо создавать специализированные

полицейские подразделения [6]. Анализ международных правовых актов по взаимовыгодному сотрудничеству в сфере противодействия киберпреступности позволил В. С. Овчинскому прийти к выводу о том, что развитие информационно-телекоммуникационных технологий и киберсреды предусматривает пересмотр основы организационно-правового функционирования правоохранительных структур, где особую роль играет использование новых технологий противодействия преступности, методов цифровых расследований, переподготовки сотрудников ведомственных органов [7, 124].

В ноябре 2000 года в г. Нью-Йорке принята Конвенция против транснациональной организованной преступности, в которой отмечена важность применения компетентными органами специальных методов расследования в целях эффективного противодействия организованной преступности. В числе таких методов названы электронное наблюдение и иные формы наблюдения, агентурные операции [8]. В свете резолюций ООН особую актуальность представляют предложения о введении в сферу уголовного судопроизводства и область оперативно-розыскной деятельности современных инструментов, позволяющих легально проводить оперативно-технические мероприятия. Так, Ю. Н. Соколов предлагает внести изменения в Федеральный закон от 12.08.1995 № 144-ФЗ «Об оперативно-розыскной деятельности» и дополнить виды оперативно-розыскных мероприятий электронным наблюдением, которое представляет собой «комплексное оперативно-техническое мероприятие, проводимое на основании судебного решения, заключающееся в конспиративном получении оперативно-техническими подразделениями субъектов оперативно-розыскной деятельности фактической или оперативно-значимой информации с помощью специальных технических средств, фиксирующих и копирующих названную информацию во время её передачи объектами оперативной заинтересованности через единые сети электросвязи Российской Федерации» [9, 14].

Успешное решение задач по противодействию преступлениям наркотической направленности, связанным с использованием компьютерных средств, обусловлено совершенствованием действующего законодательства. Особый интерес представляют Федеральные законы от 06.07.2016 № 374-ФЗ, 375-ФЗ, в обществе названные как «Пакет Ирины Яровой», предъявляющие требования к операторам связи и интернет-провайдерам сохранять информацию о телефонных звонках, сообщениях абонентов (текстовых, голосовых, видео- и иных), интернет-трафиках, декодировать сообщения

пользователей, а также предоставлять такие данные и ключи к зашифрованному трафику спецслужбам. Кроме того, были внесены существенные изменения в Федеральный закон от 07.07.2003 № 126-ФЗ «О связи», в котором операторов обязали блокировать и отключать от услуг связи лиц, анонимно использующих сотовые сети. К одному из оснований отключения абонентов от услуг связи относится пресечение преступления, которое может быть совершено с использованием телефонной связи. Данные изменения российского законодательства установили ответственность для представителей телекоммуникационных компаний за несоблюдение обязанности по идентификации своих пользователей, что положительно отразится на реализации запрета анонимного использования информационно-коммуникационной среды преступниками.

Таким образом, использование высоких технологий представителями наркобизнеса, повышение технического потенциала наркоиндустрии укрепляют преступную деятельность, расширяют наркорынок и снижают риск изобличения преступной цепи. В связи с чем, особую роль приобретают вопросы противодействия не только киберпреступлениям, но и комбинированным преступлениям, связанным с применением компьютерных и информационных технологий. Международная борьба с наркотизмом поддерживает использование различных эффективных методов противодействия этому злу, поскольку наблюдается усугубление наркоситуации и расширение процесса наркотизации населения во многих государствах. Новшества, предлагаемые на разных уровнях (выработка понятийного аппарата, перехват переписки между абонентами, верификация абонентов телекоммуникационных компаний, наложение на поставщика услуг доступа в Интернет обязательств по регистрации пользователей или фильтрации доступа на веб-сайты, трансграничный обыск, электронное наблюдение, применение программно-аппаратных средств деанонимизации, обеспечение сохранности компьютерных данных и раскрытие данных о потоках информации, проведение информационно-просветительских мероприятий среди населения) создают перспективы для совершенствования российского законодательства и науки.

Список литературы

1. Проблема наркотиков и организованной преступности, незаконные финансовые потоки, коррупция и терроризм. Всемирный доклад о наркотиках. – 2017. – Вена: Управление Организации Объединенных Наций по наркотикам и преступности, 2017. – 58 с.

2. ФСКН: наркотики стали аналогом золота для ИГ и «Боко Харам» [Электронный ресурс] // Официальный сайт Информационного агентства «РИА Новости». Режим доступа: http: ria.ru/world/20150723/114387887 (дата обращения: 30.11.2018).

3. Резюме, выводы и политические последствия. Всемирный доклад о наркотиках – 2017. – Вена: Управление Организации Объединенных Наций по наркотикам и преступности, 2017. – 45 с.

4. Литва продвигает в ЕС идею создания киберсил быстрого реагирования [Электронный ресурс] // Официальный сайт Информационного агентства «Военное обозрение». Режим доступа: http: topwar.ru/143509-litva-sozdaniya-kibersil-bystrogo-reagirovaniya(дата обращения: 30.11.2018).

5. О формировании делегации Российской Федерации для участия в работе XIII Конгресса ООН по предупреждению преступности и уголовному правосудию, проводимого в г. Доха (Катар) 12-19 апреля 2015 г.: распоряжение Правительства РФ от 10.04.2015 № 612-р //Собрание законодательства РФ. – 2015. – № 16. – Ст. 2415.

6. Доклад о работе тринадцатого Конгресса Организации Объединенных Наций по предупреждении преступности и уголовному преследованию; Доха, 12-19 апреля 2015 года [Электронный ресурс] // Официальный сайт Организации Объединенных Наций. – Режим доступа: http: www.un.org/ru/events/crimecongress (дата обращения: 30.11.2018).

7. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В. С. Овчинский. – М.: Норма, 2017. – 528 с.

8. Конвенция против транснациональной организованной преступности (принята в г. Нью-Йорке 15.11.2000 Резолюцией 55/25 на 62-ом пленарном заседании 55-ой сессии Генеральной Ассамблеи ООН) // Собрание законодательства РФ. – 2004. – № 40. – Ст. 3882.

9. Соколов, Ю. Н. Использование результатов электронного наблюдения в уголовном судопроизводстве и оперативно-розыскной деятельности: дис. ... канд. юрид. наук : 12.00.09 / Соколов Юрий Николаевич. – Екатеринбург, 2004 – 218 с.

Н.В. Володина,
доктор философских наук, доктор юридических наук, профессор Университета прокуратуры Российской Федерации, профессор кафедры судебной власти,
правоохранительной и правозащитной деятельности Российского университета дружбы народов, г. Москва

А.Г. Залужный,
доктор юридических наук, профессор, профессор кафедры правового обеспечения национальной безопасности
Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации, г. Москва

КИБЕРУГРОЗЫ СО СТОРОНЫ ЭКСТРЕМИСТСКИХ И ТЕРРОРИСТИЧЕСКИХ ОРГАНИЗАЦИЙ: ПРАВОВОЙ АСПЕКТ

Противодействие экстремизму и терроризму является одним из приоритетных направлений в деятельности прокуратуры Российской Федерации. В связи с развитием интернет-ресурсов и внедрения новых кибертехнологий, возникают проблемы для безопасности современного общества, связанные с киберугрозами, исходящими от террористических и экстремистских организаций.

Данная реальность в полной мере осознается международным сообществом. Формируется соответствующая правовая база. В качестве примера можно назвать принятую на о. Окинава 22.07.2000 г. Окинавскую хартию глобального информационного общества, в которой, в частности, заявлено, что усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства [1].

В этой связи статья 6 Модельного информационного кодекса для государств - участников СНГ [2] предусматривает ограничение законом прав и свобод в информационной сфере в интересах защиты основ конституционного строя, обеспечения национальной безопасности, защиты территориальной целостности и общественного порядка с целью предотвращения беспорядков, преступлений, разжигания социальной, расовой, межнациональной, межэтнической и религиозной вражды, др. Статья 177.1. «Склонение, вербовка или иное вовлечение в совершение преступлений террористического характера либо иное содействие осуществлению террористической

деятельности» модельного Уголовного кодекса для государств - участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере дополнена частью третьей, относящей деяния, предусмотренные частью первой или второй данной статьи, совершенные с использованием компьютерных устройств, системы или их сети, - к особо тяжким преступлениям и др. [3]

Доктрина информационной безопасности Российской Федерации (ст. 10) указывает на возможность криминального использования трансграничного оборота информации, в том числе, для достижения террористических, экстремистских и иных противоправных целей в ущерб международной безопасности и стратегической стабильности [4]. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (ст. 8) в качестве одной из основных угроз в области международной информационной безопасности называют использование информационных и коммуникационных технологий в террористических целях, в том числе для оказания деструктивного воздействия на элементы критической информационной инфраструктуры, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников [5]. При этом Федеральным законом «Об информации, информационных технологиях и о защите информации» (ст. 10.4 и ст. 10.5) запрещено использование сети «Интернет» для распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов [6].

Вышеизложенное указывает на то, что в XXI веке экстремизм и терроризм принимает все новые формы сообразно развитию современного общества и киберугрозы со стороны экстремистских и террористических организаций сегодня становятся острой проблемой для безопасности государства и его граждан. Поэтому недооценка исходящих от экстремистов и террористов киберугроз может в перспективе сказаться на безопасности не только для отдельных стран, но и мирового сообщества в целом.

Киберпространство становится для террористических и экстремистских организаций одной из важных сфер деятельности. Экстремисты и террористы применяют мобильные системы, коммуникационные сети и современные информационные технологии. Один из ярких и известных тому примеров - террористическая атака в Мумбае (ранее Бомбей, мегаполис на западном побережье Индии) в

2008 году. Террористы группировки «Лашкар-э-Тайба» пользовались системами GPS и 3G для подготовки и проведения нападения на гражданские объекты, используя смартфоны для сбора информации об объектах, обеспечения связи между преступниками и осуществления тактического руководства боевиками во время нападения. Существует реальная опасность то, что компьютерные технологии, используемые экстремистскими организациями и террористическими группировками пока только как вспомогательные средства для проведения террористического акта, в ближайшем будущем станут основным звеном в организации террористической деятельности, включая управление вооружением и боевой техникой. К такому сценарию развития событий мир должен быть готов.

Вместе с усложнением технологий неизбежно появляются и новые возможности их использования в преступных целях. В этом смысле вызывает тревогу информация эксперта Positive Technologies Бориса Симиса редакции портала «Безопасность пользователей в сети Интернет», из которой следует, что, как считают специалисты, при помощи кибератак могут быть взломаны даже хорошо защищенные инфраструктуры.[7]Не исключено, что кибератаки могут быть осуществлены в террористических целях. Сегодня экстремистские и террористические организации активно используют киберпространство для распространения идеологии терроризма в информационно-коммуникационных сетях и вербовки сторонников,[8] а завтра они смогут применять в своих целях новые сложные технологии, представляя тем самым угрозу национальной безопасности любой страны. Учитывая ситуацию на Ближнем Востоке и странах Западной Европы, куда хлынули мигранты из исламских стран, *кибератаки скорее можно считать как акт войны начальной стадии* в создавшихся условиях при бурном развитии компьютерных технологий, которые легко осваивают, например, исламские экстремисты.

Понимание данной проблемы в мире есть. В США, например, не просто серьезно занимаются вопросами кибербезопасности, но и проводят отдельные *учения кибервойск.* Киберугрозы в США рассматриваются с двух позиций: во-первых, как угроза национальной безопасности; во-вторых, как угроза общественной безопасности, включающая в основном экономические вопросы. Противодействие киберугрозам, угрожающим национальной безопасности США (в том числе исходящим от экстремистских и террористических организаций), осуществляется на государственном уровне; борьба с такими проявлениями носит систематический характер с выделением

должного количества финансовых ресурсов. При этом сами США многие специалисты рассматривают в «качестве источника угрозы кибернетической и в целом национальной безопасности России и других стран» в силу фактического регулирования ими сети Интернет за счет реального управления «практически всем адресным пространством DNS (доменной системы имен)» [9].

Принятая Советом Европы «Конвенция о преступности в сфере компьютерной информации» (Заключена в г. Будапеште 23.11.2001(с изм. от 28.01.2003) устанавливает (ст.2 Противозаконный доступ) что каждая Сторона принимает законодательные и иные меры, необходимые для того, чтобы квалифицировать в качестве уголовного преступления согласно ее внутригосударственному праву доступ, когда он является преднамеренным, к компьютерной системе и др.Однако этот документ не содержит упоминания о возможности киберугроз со стороны экстремистских и террористических организаций, что, на наш взгляд, ограничивает ее рамки формальной констатацией проблемы и не содержит достойный ответ на особо острые негативные вызовы современности.

С другой стороны «Шанхайская конвенция о борьбе с терроризмом, сепаратизмом и экстремизмом» (Заключена в г. Шанхае 15.06.2001), признавая экстремизмом какое-либо деяние, направленное на насильственный захват власти или насильственное удержание власти, а также на насильственное изменение конституционного строя государства, а равно насильственное посягательство на общественную безопасность, в том числе организация в вышеуказанных целях незаконных вооруженных формирований или участие в них, и преследуемые в уголовном порядке в соответствии с национальным законодательством Сторон, со всей ясностью указывает на него как угрозу международной безопасности.

В то же время вопросы противодействия кибератакам террористических и экстремистских группировок Шанхайской организацией сотрудничества тоже не затрагивались и единой модели противодействия киберпреступности до сих пор не существует, что, возможно, связано с тем, что это явление стало известно лишь в 90-х годах XX века и еще не сложилось понимание важности этой проблема для многих государств.

В этой связи Директор ФСБ России считает, что террористам играет на руку анонимность в Интернете, технический уровень и изощренность кибератак с их стороны постоянно растут, кроме того, экстремисты пользуются интернет-ресурсами для распространения своих идей и вовлечения в группировки новых членов [10].

Так, распространение исламских экстремистских и террористических групп не ограничивается территорией Северного Кавказа, а наблюдается во многих регионах России. Например, по данным правоохранительных органов в 2018 году, в Норильске задержана группа экстремистов, вербовавших новых сторонников в ИГ («Исламское государство» - террористическая группировка, запрещенная на территории России), которые принимали активное участие в финансировании терроризма и публично призывали к экстремистской и террористической деятельности. Подобные проявления отмечены в Красноярском крае. В Твери вынесен обвинительный приговор уроженцу Центральной Азии, причастному к финансированию международной террористической организации. В мае 2018 года в г. Ярославле задержаны пять членов другой террористической ячейки ИГ, готовившей организацию терактов на территории целого ряда субъектов РФ. Координация подготовки к совершению терактов осуществлялась посредством мессенджера Telegram, в том числе из-за рубежа. В марте 2018 года признательные показания в подготовке терактов дали пятеро задержанных в Калужской области участников ячейки ИГ, признавшихся, что получили задание совершить теракт.

При этом эффективное противодействие экстремистам и террористам предполагает также использование экспертов, обладающих специальными знаниями в различных отраслях науки и техники. В этой связи, на наш взгляд, правовой проработки в России и в других государствах, включая международные нормативные правовые акты, требует защита экспертов от «*кибердиффамации*» (от лат. «порочить»), когда посредством сети Интернет распространяются недостоверные сведения, нарушающие их достоинство, честь и деловую репутацию. От таких нападок специалисты, занимающиеся проблемами противодействия экстремизму и терроризму, фактически не защищены, а экстремисты активно используют киберпространство для дискредитации ученых, других специалистов и сотрудников правоохранительных органов. В России сегодня защиты от такого рода деятельности нет.

В связи с вышеизложенным следует отметить, что подтверждается тесная связь киберпреступности с такими опасными видами преступлений как экстремизм и терроризм и существуют опасения, что экстремистские и террористические организации имеют доступ к современным компьютерным технологиям используются услугами высокопрофессиональных специалистам в этой сфере. Большую опасность представляют как сами хакеры, так и связанные с

ними члены преступных экстремистских и террористических группировок. По мнению А.С. Линникова, «с одной стороны, деятельность «системных» хакеров ограничена их руководством, но с другой - они получают доступ к значительным ресурсам, а в случае с терроризмом могут быть нацелены на решение задач по нанесению максимального ущерба противнику, в том числе путем разрушения жизненно важных систем, совершения терактов с множеством человеческих жертв» [11].

Это можно отнести и к экстремистским организациям, учитывая, что их последователи, в особенности ориентированные на радикальный ислам, постепенно распространяются по территории России, вербуя новых сторонников. Имея достаточные финансовые ресурсы и учитывая низкооплачиваемость специалистов в стране, особенно в регионах, они находят людей, владеющих компьютерными технологиями и готовых по материальным соображениям вступить в преступный сговор с членами экстремистских и террористических групп.

Сегодня преступные организации используют разные изощренные технологии, о чем свидетельствуют резко возросшее число хакерских взломов, имитация внешности человека по данным из социальной сети и утечки личных сведений. Как указывает компания Group-IB, в 2017 годукиберпреступники 20 раз подвергали хакерским атакам банки США, России, Великобритании. Вычислить таких преступников крайне сложно. По оценкам экспертов, в среднем ущерб от одной такой атаки для США - 500 тыс. долл., для России - 72 млн. руб. То есть, информация о каждом человеке, в том числе биометрические персональные данные доступны. Таким образом, тех, кто неудобен экстремистам и террористам легко «вычислить» и использовать информацию в негативных целях, применяя компьютерные технологии.[12]

Количество киберпреступлений выросло на 75%, отмечается в программе «Цифровая экономика Российской Федерации». По данным Генерального прокурора России Ю. Чайки, число киберпреступлений в России в 2017 г. по сравнению с 2013 г. увеличилось в шесть раз. В 2016 г. было зарегистрировано 66 тысяч IT-преступлений (в 2013 г. этот показатель составлял 11 тысяч) [13]. Отдельного статистического учета киберпреступлений экстремистской и террористической направленности в настоящее время нет, что затрудняет анализ проблем этого направления. При этом, по мнению специалистов, Интернет стал серьезным оружием в руках деструктивных элементов, которые используют его для распространения незаконной информации, в том

числе побуждающей других участников интернет-пространства к совершению действий, направленных на нарушение территориальной целостности России, либо формирующей в их умах позицию об обоснованности и оправданности свершения таких действий [14].

Таким образом, вопросы кибербезопасности, в особенности в сфере противодействия экстремизму и терроризму, нуждаются в дальнейших научных исследованиях и законодательном регулировании.

В частности, Федеральным законом от 29.07.2017 № 241-ФЗ «О внесении изменений в статьи 10.1 и 15.4 Федерального закона «Об информации, информационных технологиях и о защите информации» установлена обязанность идентификации пользователей по абонентскому номеру при передаче электронных сообщений с использованием сервиса обмена мгновенными сообщениями (мессенджера), непосредственно направленная на противодействие экстремистским проявлениям в Интернете.

Федеральным законом от 25.11.2017 № 327-ФЗ «О внесении изменений в статьи 10.4 и 15.3 Федерального закона «Об информации, информационных технологиях и о защите информации» и статью 6 Закона Российской Федерации «О средствах массовой информации» дополнен перечень информации, распространяемой с нарушением закона, предусмотренный ч. 1 ст. 15.3 Федерального закона от 27.07.2006 № 149-ФЗ информационными материалами иностранной или международной неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации. Это дало возможность ограничения доступа к интернет-сайтам организаций, признанных в России нежелательными.

В то же время ряд специалистов высказывает сомнение в эффективности принятых мер для противодействия киберугрозам со стороны экстремистских и террористических организаций. В частности, высказывается мнение о том, что «хранение данных на территории России без регулярного анализа трафика едва ли сможет со стопроцентной вероятностью предотвратить кибератаку и в целом обеспечить кибербезопасность на национальном уровне» [15] и др.

Все это говорит о том, что понимание важности проблемы есть и у государства в лице его субъектов обеспечения кибербезопасности, и у гражданского общества.

Для ее решения, на наш взгляд, необходимо разработать концепцию кибербезопасности в сфере противодействия экстремистским и террористическим киберугрозам не формально, а с использованием инноваций и привлечением профессиональных

научных кадров и практических работников для выработки стратегии, опережающей развитие компьютерных и других высоких технологий.

Список литературы

1. Дипломатический вестник. 2000. № 8. С. 54.
2. Принят в г. Санкт-Петербурге 23.11.2012 Постановлением № 38-6 на 38-ом пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ.
3. Приняты в г. Санкт-Петербурге 27.11.2015 Постановлением 43-16 на 43-ем пленарном заседании Межпарламентской Ассамблеи государств-участников СНГ.
4. «Собрание законодательства РФ», 12.12.2016, № 50, ст. 7074.
5. Утверждены Президентом РФ 24.07.2013 № Пр-1753.
6. Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 19.07.2018).
7. https://uzsoft.uz/эксперт-positive-technologies-рассказал-о-новых-векторах-атак/ 21.03.2018.
8. Противодействие вербовочной деятельности международных террористических организаций на территории Российской Федерации: пособие / [А.С. Васнецова, В.В. Меркурьев, Д.А. Соколов и др.]; Акад. Ген. прокуратуры Рос. Федерации. – М., 2017; Деятельность органов прокуратуры по предупреждению преступлений против основ конституционного строя и безопасности государства: пособие / П.В. Агапов и др. Акад. Ген. прокуратуры Рос. Федерации. М., 2017.– С. 44, 76, 83.
9. Тонконогов А.В. Кибернетическая безопасность: понятие и сущность феномена // Право и кибербезопасность. 2013. № 2. С. 36 - 43.
10. В. Маслова, П.Астахов. Стратегия экстремистов: глава ФСБ рассказал о планах ИГ создать новую террористическую сеть // https://ru.rt.com/9crx. 4 октября 2017.
11. Линников А.С. Экономические последствия расширения масштабов киберпреступности в России и мире // Банковское право. 2017. № 5. С. 19 - 29.
12. Хакерская группировка MoneyTaker опустошает банки США и России// https://newdaynews.ru/technology/622809.html. Дата обращения: 11.12.2017
13. Алиев В.М., Соловых Н.Н. Цифровая экономика поставила нас перед необходимостью решения проблемы обеспечения цифрового суверенитета // Безопасность бизнеса. 2018. № 3. С. 18 - 22.

14. Деятельность органов прокуратуры по предупреждению преступлений против основ конституционного строя и безопасности государства: пособие / [П.В. Агапов и др.]; Акад. Ген. прокуратуры Рос. Федерации. – М., 2017. – 128 с.

15. Двенадцатова Т. Новый год под знаком запрета // ЭЖ-Юрист. 2017. № 50. С. 5.

И.Т. Гасанов,
преподаватель кафедры уголовного процесса и криминалистики Пермский государственный национальный исследовательский университет, г. Пермь

К ВОПРОСУ О ПОЛУЧЕНИИ СУДЕБНОГО РАЗРЕШЕНИЯ НА ОСМОТР СОТОВЫХ ТЕЛЕФОНОВ УЧАСТНИКОВ УГОЛОВНОГО ПРОЦЕССА НА ДОСУДЕБНЫХ СТАДИЯХ

В статье раскрываются противоречивые подходы ученых, сотрудников правоохранительных органов, а также судов общей юрисдикции в вопросе о необходимости получения ***судебного разрешения*** для осмотра мобильных телефонов и содержащейся в них информации участников уголовного судопроизводства. В связи с определениями Конституционного Суда РФ от 25.01.2018 № 189-О [1], а также от 17.07.2018 № 1955-О [2] автор настоящей статьи выражает озабоченность, в том, что позиция, изложенная в вышеуказанных определениях, может привести к незаконному ограничению конституционного права на тайну переписки.

На сегодняшний день в УПК РФ [3] остается нерешенным вопрос о том, следует ли сотрудникам правоохранительных органов получать ***судебное разрешение*** на осмотр мобильных телефонов и содержащейся в них информации участников уголовного судопроизводства (сообщений электронной почты, ММС, СМС, сообщения в приложениях Viber, WatsApp и др.). Указанный вопрос не нашел своего разрешения и в разъяснениях Пленума Верховного Суда РФ. В частности, Пленум Верховного Суда РФ, обращаясь к данной проблеме, не обратил внимания на этот аспект в Постановлении от 01.06.2017 г. № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением

конституционных прав граждан (статья 165 УПК РФ)» [4].

Следует отметить, что и среди ученых остается дискуссионным вопрос о том следует ли получать судебное разрешение для осмотра мобильных телефонов, а также по вопросу о том, с какой информацией, содержащейся в памяти мобильного телефона, сотрудники правоохранительных органов имеют право знакомиться без судебного разрешения.

С.В. Зуев, ссылаясь на американский опыт, полагает, что «в связи с неоднозначной правовой оценкой действий, связанных с осмотром мобильных телефонов, представляется необходимым в УПК определить основания ограничения конституционных прав физических лиц в конкретных случаях» [5].

А.Н. Яковлев применительно к сообщениям электронной почты считает, что пока сообщение находится на компьютерном средстве пользователя, такие данные не являются тайной связи. Как только правообладатель коммуникационного сервиса «Мэйл.Ру», «Яндекс» или др. получает эти данные, пересылает оператору связи, данные являются электронными сообщениями или электронной почтой, охраняемой тайной связи. Будучи доставленными получателю, т.е. на компьютерное средство пользователя, они вновь становятся не охраняемыми законом данными, которые получил пользователь сети Интернет. В этой связи, автор делает вывод, что возможно «получать информацию в порядке ст. 86 УПК РФ в ходе следственных действий... Решения суда при этом также не требуется» [6].

Практика органов предварительного расследования показывает, что нередко на досудебных стадиях следователи, дознаватели изымают и осматривают мобильные телефоны подозреваемых, свидетелей, потерпевших без какого-либо судебного разрешения. Вместе с тем, обращает на себя особое внимание, что указанные действия совершаются сотрудниками правоохранительных органов вне зависимости от того, какое преступление совершено, каким способом, а также не выясняются отношение (согласие) участников на производство такого осмотра.

По мнению Р.Г. Бикмиева, Р.С. Бурганова «получение доступа к информации, содержащейся в мобильном телефоне (ином электронном устройстве), и использование этой информации оперативными работниками или следователем также следует считать преступлением, если такие действия осуществлены без получения судебного разрешения и повлекли общественно опасные последствия. В зависимости от обстоятельств дела данные деяния могут быть квалифицированы как злоупотребление должностными полномочиями

(ст. 285 УК РФ), превышение должностных полномочий (ст. 286 УК РФ) или нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ)» [7].

А.М. Багмет, С.Ю. Скобелин считают, что обнаружение, фиксация, изъятие и сохранение информации, содержащейся в памяти мобильных телефонов, таких как список контактов, исходящие и входящие звонки, ММС, СМС-сообщения, загруженные файлы, история посещения различных сайтов в интернете через телефон, фотографии и видеозаписи в галерее и др., зачастую способствует своевременному изобличению лиц, причастных к совершению преступления, оперативному их розыску и задержанию, определения места нахождения трупов, похищенного имущества, место нахождения похищенных лиц, орудия преступления и т.д., что в свою очередь обеспечивает сторону обвинения надежной доказательственной базой. В то же время, указанные ученые приходят к выводу, что в ситуациях, когда сотовый телефон участника уголовного судопроизводства изъят и находится у следователя, получать судебное решение на его осмотр и ознакомление с цифровым содержимым не требуется [8].

Вместе с тем, как правильно отмечает Р.И. Оконенко, существующее российское уголовно-процессуальное законодательство не выработало необходимых ***процессуальных гарантий для защиты граждан*** от чрезмерного интереса со стороны публичной власти [9].

Судебная практика также неоднозначна в разрешении обсуждаемой проблемы [10,11].

Высокотехнологичные устройства, которые используются в отделах криминалистики следственных управлений Следственного комитета РФ при осмотре мобильных телефонов (аппаратно-программные комплексы UFED, комплекс XRY и др.) позволяют извлечь и систематизировать удаленные данные, объединить дампы памяти, извлеченные из нескольких телефонов, проследить особенности и структуру связи проверяемых лиц, данные вызовов IP-телефонии, картографическую информацию GPS и журналы средств оперативной пересылки сообщений [12].

Однако, если проблем с собственно изъятием мобильных телефонов как на стадии возбуждения уголовного дела, так и в ходе предварительного расследования у практических работников не возникает, то вопросы, связанные с изучением (осмотром) информации, содержащейся в памяти мобильных телефонов, пределов ознакомления с такой информацией в отсутствие специального судебного разрешения, остаются открытыми и дискуссионными.

По рассматриваемой проблеме высказался и Конституционный Суд РФ. Так, в Определении от 25.01.2018 № 189-О Конституционный Суд РФ пришел к выводу, что ***проведение осмотра и экспертизы с целью получения имеющей значение для уголовного дела информации, находящейся в электронной памяти абонентских устройств***, изъятых при производстве следственных действий в установленном законом порядке, ***не предполагает вынесения об этом специального судебного решения***. Лица же, полагающие, что проведение соответствующих следственных действий и принимаемые при этом процессуальные решения способны причинить ущерб их конституционным правам, в том числе праву на тайну переписки, почтовых, телеграфных и иных сообщений, могут оспорить данные процессуальные решения и следственные действия в суд в порядке, предусмотренном статьей 125 УПК РФ. В последующем, в Определении от 17.07.2018 № 1955-О Конституционный Суд РФ подтвердил свою правовую позицию, изложенную в Определении от 25.01.2018 № 189-О. Однако представляется, что такая позиция Конституционного Суда РФ о возможности ознакомления с информацией, содержащейся в памяти мобильных телефонов без судебного разрешения, противоречит ранее изложенным правовым позициям Конституционного Суда РФ, в частности в определениях от 02.10.2003 № 345-О [13] и от 21.10.2008 № 528-О-О [14].

Из Определения Конституционного Суда РФ от 02.10.2003 № 345-О следует, что наделение суда полномочием осуществлять независимую оценку действий правоохранительных органов, связанных с ограничением конституционных прав граждан (***в том числе право на тайну переписки – добавлено мной И.Т.***), создает дополнительные условия защиты этих прав. Поэтому полнота использования данного полномочия является важнейшей предпосылкой упрочения норм жизни правового государства. Конституция Российской Федерации, устанавливая основания применения судебного контроля, определяет его основные параметры, исключающие возможность как ограничительного, так и расширительного истолкования его предмета и сферы действия.

При этом Конституционный Суд РФ указал, что право каждого на тайну телефонных переговоров по своему конституционно-правовому смыслу предполагает комплекс действий по защите информации, получаемой по каналам телефонной связи, независимо от времени поступления, степени полноты и содержания сведений, фиксируемых на отдельных этапах ее осуществления; в силу этого к информации, составляющей охраняемую Конституцией Российской

Федерации и действующими на территории Российской Федерации законами тайну телефонных переговоров, ***относятся любые сведения, передаваемые, сохраняемые и устанавливаемые с помощью телефонной аппаратуры***, включая данные о входящих и исходящих сигналах соединения телефонных аппаратов конкретных пользователей связи. ***Для доступа к указанным сведениям необходимо получение судебного решения***.

В Определении от 21.10.2008 Конституционный Суд РФ фактически воспроизвел содержание своего же Определения от 02.10.2003 № 345-О.

Таким образом, попытаемся внести ясность в понимании вопроса необходимо ли получать судебное разрешение на осмотр мобильных телефонов и содержащейся в них информации участников уголовного судопроизводства, а также выразим свое отношение к правовым позициям Конституционного Суда РФ, изложенным в определениях от 25.01.2018 № 189-О, а также от 17.07.2018 № 1955-О.

Во-первых, Уголовно-процессуальный кодекс РФ прямо не предусматривает обязанность следователя (дознавателя) получать ***судебное разрешение*** на осмотр мобильных телефонов и содержащейся в них информации участников уголовного судопроизводства (сообщений электронной почты, ММС, СМС, сообщения в приложениях Viber, WatsApp и др.). Однако это вовсе не означает, что такой обязанности у следователя не имеется, такая обязанность вытекает, в частности из норм УПК РФ (ст. 13), Конституции РФ (ч. 2 ст. 23), а также Конвенции о защите прав человека и основных свобод (ст. 8) [15]. Безусловно, вышеуказанные нормы российского, а также международного права предполагают защиту тайны на переписку, телефонных переговоров, почтовых, телеграфных и иных сообщений. При этом необходимо получение следователем (дознавателем) судебного разрешения на производство осмотра мобильных телефонов и содержащихся в мобильных телефонах информации.

Во-вторых, ММС, СМС, мгновенные сообщения через приложения Viber, WatsApp, сообщения через социальные сети «Вконтакте», «Одноклассники» и др. имеют ***двусторонний характер*** и содержит мысли не только подозреваемого, обвиняемого, потерпевшего, но и других лиц, пусть и имеющих (может, вообще не имеющих) отношение к делу, но никак не извещенных о том, что их личная переписка, обмен различными фотографиями, файлами, видеозаписями и др. будут известны следователю (дознавателю).

В-третьих, при осмотре мобильных телефонов должностные

лица органов предварительного расследования ограничивают конституционное право гражданина на тайну личной переписки не только без его согласия, но и без судебного разрешения.

В-четвертых, разделяем точку зрения тех ученых, которые полагают, что в ходе осмотра мобильных телефонов происходит фактически обыск [16].

Как известно, под осмотром понимается визуальное обследование предмета без активных поисковых действий, присущих обыску. Поэтому, как справедливо отмечает О.В. Добровлянина, если необходимо исследовать сведения, содержащиеся в папках с файлами (в компьютере, мобильном телефоне и др.), т.е. провести целенаправленный активный поиск информации, аналогичный обыску, то выработанное практикой устоявшееся название осмотр компьютера, мобильного телефона не вполне отражает суть этого сложного процессуального действия. Очевидно, вряд ли будет правильным фактически провести обыск, но оформить действие как осмотр [17].

Таким образом, во избежание необоснованного вмешательства органов предварительного расследования в личную жизнь граждан, фактической замены одного следственного действия другим (осмотра обыском), а также во избежание ошибок со стороны практических работников в выборе следственного действия считаем, что необходимо внести следующие изменения в УПК РФ:

- дополнить п. 4.1 ч. 2 ст. 29 и изложить его в следующей редакции: «о производстве осмотра электронных устройств, в т.ч. мобильных телефонов, компьютеров, планшетов с целью изъятия и обработки персональных данных при отсутствии согласия субъектов персональных данных»;

- ч. 5 ст. 165 после слов «личного обыска» дополнить фразой «осмотра электронных устройств, в т.ч. мобильных телефонов, компьютеров, планшетов с целью изъятия и обработки персональных данных»;

Вместе с тем, в связи с особенностями вышеуказанного следственного действия, полагаем, что необходимо ввести в УПК РФ новую статью, которая бы регламентировала основания и порядок его производства.

Список литературы

1. Определение Конституционного Суда РФ от 25.01.2018 № 189-О «Об отказе в принятии к рассмотрению жалобы гражданина Прозоровского Дмитрия Александровича на нарушение его конституционных прав статьями 176, 177 и 195 Уголовно-

процессуального кодекса Российской Федерации». [Электронный ресурс] // СПС «КонсультантПлюс».

2. Определение Конституционного Суда РФ от 17.07.2018 № 1955-О «Об отказе в принятии к рассмотрению жалобы гражданина Сидака Константина Петровича на нарушение его конституционных прав частью шестой статьи 164 и статьей 177 Уголовно-процессуального кодекса Российской Федерации». [Электронный ресурс] // СПС «КонсультантПлюс».

3. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (ред. от 30.10.2018) // Собрание законодательства РФ. 24.12.2001. № 52 (ч. I). Ст. 4921.

4. Постановление Пленума Верховного Суда РФ от 01.06.2017 № 19 «О практике рассмотрения судами ходатайств о производстве следственных действий, связанных с ограничением конституционных прав граждан (статья 165 УПК РФ)» // Российская газета. № 125. 09.06.2017.

5. Зуев С.В. Осмотр и изъятие электронных носителей информации при проведении следственных действий и оперативно-розыскных мероприятий // Законность. 2018. № 4. С. 58-60.

6. Яковлев А.Н. Правовой статус цифровой информации, извлекаемой из компьютерных и мобильных устройств: «электронная почта» // Вестник Воронежского института МВД России. 2014. № 4. С. 42-48.

7. Бикмиев Р.Г., Бурганов Р.С. Выемка и осмотр электронных устройств // Уголовное право. 2018. № 1. С. 125-131.

8. Багмет А.М., Скобелин С.Ю. Пределы ограничения конституционных прав граждан в ходе осмотра сотовых телефонов участников уголовного судопроизводства // Уголовное право. 2017. № 6. С. 97-103.

9. Окоменко Р.И. Электронные доказательства как новое направление совершенствования российского уголовно-процессуального права // Актуальные проблемы российского права. 2015. № 3. С. 120 - 124.

10. Апелляционное постановление Приморского краевого суда от 02.02.2015 по делу № 22К-455/2015. [Электронный ресурс] // СПС «КонсультантПлюс». Дата обращения: 26.11.2018.

11. Апелляционное определение Верховного Суда РФ от 11.10.2016 № 32-АПУ16-12. [Электронный ресурс] // СПС «КонсультантПлюс».

12. Бутенко О.С. Криминалистические и процессуальные аспекты проведения осмотра мобильных телефонов в рамках предварительного следствия // Lex russica. 2016. № 4. С. 49 - 60.

13. Определение Конституционного Суда РФ от 02.10.2003 № 345-О «Об отказе в принятии к рассмотрению запроса советского районного суда города Липецка о проверки конституционности части четвертой статьи 32 Федерального закона от 16 февраля 1995 года «О связи» // Российская газета, № 250, 10.12.2003.

14. Определение Конституционного Суда РФ от 21.10.2008 № 528-О-О «Об отказе в принятии жалоб гражданина Муллина Александра Анатольевича на нарушение его конституционных прав положениями статьи 9 Федерального закона «Об информации, информационных технологиях и о защите информации» и статьи 53 Федерального закона «О связи». [Электронный ресурс] // СПС «КонсультантПлюс».

15. Конвенция о защите прав человека и основных свобод, заключена в г. Риме 04.11.1950 (с изм. от 13.05.2004) (вместе с «Протоколом [№ 1]» (Подписан в г. Париже 20.03.1952), «Протоколом № 4 об обеспечении некоторых прав и свобод помимо тех, которые уже включены в Конвенцию и первый Протокол к ней» (Подписан в г. Страсбурге 16.09.1963), «Протоколом N 7» (Подписан в г. Страсбурге 22.11.1984)).

16. Черкасов В.С. Значение дифференциации следственных действий «осмотр» и «обыск» при исследовании компьютерной информации // Актуальные вопросы рассмотрения уголовных дел в суде присяжных: сборник материалов Всероссийской научно-практической конференции / Е.Ю. Антонова, Е.В. Арцева, С.С. Безруков и др.; под ред. С.С. Безрукова, К.А. Волкова. Хабаровск: Юрист, 2017. 104 с.

17. Добровлянина О.В. К вопросу о системе следственных действий в уголовном судопроизводстве // Седьмой Пермский конгресс ученых-юристов (г. Пермь, 18 - 19 ноября 2016 г.): сборник научных статей / В.В. Акинфиева, Л.А. Аксенчук, А.А. Ананьева и др.; отв. ред. В.Г. Голубцов, О.А. Кузнецова. М.: Статут, 2017. 592 с.

С.А. Горовой,
ассистент кафедры уголовного процесса и криминалистики
Алтайский государственный университет», г. Барнаул

В.Ю. Деминова,
преподаватель колледжа
Алтайский государственный университет, г. Барнаул

МОШЕННИЧЕСТВО С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА: ПРАВОВЫЕ ПРОБЛЕМЫ ПРОТИВОДЕЙСТВИЯ

Все большее распространение в обществе имеет тенденция к совершению безналичных расчетов в повседневной жизни: получение заработной платы, осуществление платежей посредством банковской карты, терминала, осуществление расчетов платежными поручениями. В то же время с развитием в стране экономических отношений, информационных технологий появляются новые виды преступлений против собственности, имеющие свою специфику квалификации. Одним из нововведений уголовного закона стала дифференциация мошенничества. Появилось мошенничество с использованием платежных карт (ст. 159.3 УК РФ) в качестве самостоятельного состава преступления, под которым понималось хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации [1]. В соответствии с Федеральным законом от 23 апреля 2018 г. № 111-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» данная статья УК РФ получила следующее наименование – «мошенничество с использованием электронных средств платежа» [2].

Платежная карта в современном мире является самым распространенным средством платежа, она предоставляет доступ к собственному счету. О распространенности платежных карт свидетельствуют статистические данные, предоставленные Центральным банком Российской Федерации. По состоянию на 1 января 2018 г. всего эмитировано кредитными организациями 271 005 тыс. единиц платежных карт (по состоянию на 1 октября 2017 г. эмитировано 267 219 тыс. единиц) [3].

Преимущества платежных карт очевидны – удобство в применении, сохранение в случае утраты карты денежных средств.

Вместе с тем появление платежных карт способствовало активизации деятельности тех лиц, которые знают слабые места системы платежей. Конечно, по сравнению с иными формами хищения доля лиц, осужденных по ст. 159.3 УК РФ, остается незначительной [4], однако нельзя недооценивать общественную опасность преступлений в указанной сфере. Мошенничество при расчетах платежными картами распространяется стремительно сообразно увеличению эмитированных платежных карт. Если принять во внимание сведения, полученные из Испании, Германии и России, то суммарно получится 80% всех преступлений мира в области использования платежных карт. Кроме того, существуют данные, что в 2013 г. совокупный ущерб от мошенничества с использованием платежных карт в 19 европейских странах составил 1,55 миллиарда евро. В последующие годы ущерб оставался на том же уровне [5].

Рост мошенничества в данной сфере связан с недостаточной защищенностью рынка электронных платежей, а также с распространенностью магнитных карт, которые менее защищены от неправомерного доступа, чем карты с чипами. Кроме того, транзакции с платежными картами могут осуществляться без непосредственного посещения кредитной, торговой или иной организации, а при определенных условиях и без непосредственного использования самой платежной карты. На сегодняшний день около 80% обращений через Интернет-сайт МВД РФ посвящаются мошенничеству при покупке товаров через социальные сети и интернет-магазины посредством электронной оплаты. Также совершенствуются и вредоносные программы для мобильных устройств в целях получения доступа к мобильному банку потерпевшего и к его конфиденциальным сведениям. Учитывая данные тенденции, законодателем было принято решение о модернизации российского уголовного законодательства в соответствии с требованиями, предъявляемыми информационным сообществом.

Предметом мошенничества с использованием электронных средств платежа является чужое имущество, а именно денежные средства, находящиеся на счете. Сами электронные средства платежа выступают в качестве средства, дающего возможность получения указанных денежных средств, либо оплаты с их помощью товаров и услуг.

Федеральный закон «О национальной платежной системе» от 27 июня 2011 г. № 161 позволяет трактовать понятие «электронного средства платежа» шире, чем «платежная карта» и «банковская карта» [6]. Так, в силу п. 17 ст. 3 указанного закона платежная услуга – это

услуга по переводу денежных средств, услуга по приему платежей, услуга почтового перевода. Под электронным средством платежа понимается средство и (или) способ, позволяющие клиенту оператора по переводу денежных средств составлять, удостоверять и передавать распоряжения в целях осуществления перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации, в том числе платежных карт, а также иных технических устройств. Указанные положения позволяют предположительно относить к платежным инструментам и иные, кроме платежных, виды карт, в частности дисконтные карты, сертификаты, подарочные карты, приобретенные у коммерческих организаций, отражающие номинальную стоимость, принимаемые к оплате указанными организациями. Вместе с тем некоторые исследователи, например, С.М. Кочои [7, С. 37], подобные карты относят к категории торговых, которые, на их взгляд, не могут рассматриваться в рамках мошенничества, предусмотренного ст. 159.3 УК РФ.

Чтобы разрешить указанную проблему, следует обратиться к нормативным актам, регламентирующим порядок эмиссии платежных карт и осуществления операций с их использованием [8]. Так, в «Положении об эмиссии платежных карт и об операциях, совершаемых с их использованием» понятие платежной карты отсутствует, но даются определения различных ее разновидностей (расчетная (дебетовая), кредитная, предоплаченная карта). Системное сравнение данных определений позволило сделать вывод, что главным признаком платежной карты является ее платежная способность, то есть возможность осуществления операций с денежными средствами с ее помощью. Значит, различные социальные карты только в некоторых случаях можно отнести к числу возможных средств совершения с их помощью мошенничества – если они пригодны для реализации расчетов. К примеру, карты москвича выпускаются с банковским приложением, которое позволяет осуществлять денежные операции. Различные дисконтные, бонусные, топливные карты для этого непригодны, соответственно, средством преступления, предусмотренного ст. 159.3 УК РФ, являться не могут.

Федеральным законом от 23 апреля 2018 г. №111-ФЗ «О внесении изменений в Уголовный Кодекс Российской Федерации» была фактически расширена сфера применения рассматриваемой нормы. Платежные карты наряду с иными электронными средствами платежа становятся средствами совершения преступления,

предусмотренного ст. 159.3 УК РФ. В указанном аспекте важно помнить, что «платежная карта» и «банковская платежная карта» – это не тождественные явления, поскольку существуют сервисы (например: Qiwi, WebMoney, Яндекс Деньги и т.д.), не являющиеся банками, но предоставляющие услугу по оплате товаров. Такие сервисы могут оказывать услуги по созданию «виртуальной платежной карты», которая обладает многими признаками банковской карты, за исключением следующего: она не существует на материальном носителе. Следовательно, вопрос об отнесении к средствам мошенничества, предусмотренного ст. 159.3 УК РФ, Qiwi, WebMoney, Яндекс.Деньги и т.д. может быть снят в пользу причисления их к иным средствам.

Несмотря на то, что в действующей редакции ч. 1 ст. 159.3 УК РФ об этом прямо не говорится, на наш взгляд, для рассматриваемого состава преступления имеет значение состояние платежной карты (и других электронных средств платежа): она должна быть поддельной или принадлежащей другому лицу. На примере платежной карты под принадлежащими другому лицу картами понимаются те, что ранее были похищены, найдены, получены путем вымогательства, а также те, что были добровольно переданы владельцем, но для расходования меньшей суммы [9, С. 48-51].

Поддельной является карта, полностью воссоздающая аналог подлинной карты, а также подлинная карта, измененная частично (скорректированы реквизиты, информация на магнитном носителе или на лицевых сторонах карты и т. п.). Способы подделки могут быть разнообразными.

Способом подделки могут выступать примитивные фальшивые карточки. На заготовку наносится логотип эмитента, поле для проставления подписи держателя карты, повторяются степени защиты. Фальшивые карточки внешне настолько схожи с оригиналом, что уполномоченный работник кредитной, торговой или иной организации вряд ли сможет заметить подделку.

В рамках данного способа возможна и частичная подделка. Виновное лицо изменяет некоторые реквизиты – например, номер, фамилию держателя карты. Информация о счете удаляется (механическим, термическим способом) на карточке, а на место этой информации наклеивается новый номер, вырезанный с другой карточки. Таким образом, товар приобретается, но не оплачивается.

Еще одним способом подделки является изготовление специального считывающего устройства на банкомате. Устройства устанавливаются на клавиатуру банкомата и позволяют запоминать

все нажатые комбинации кнопок, а информацию о номере карты, о ее владельце считывают заранее установленные считывающие механизмы [10, С. 589–593].

Способом завладения картой может быть «свой банкомат». Данная разновидность мошенничества представляет собой установку конверта, который по размерам немного больше карты. Когда держатель платежной карты совершает попытку снять деньги в банкомате, тот не может прочесть данные магнитной полосы. В этом случае держатель карты запрашивает ее назад, но банкоматом данная функция не может быть выполнена, поскольку конструкция конверта не позволяет изъять карточку из банкомата обратно. Далее владелец думает, что карта осталась в банкомате, и уходит с тем, чтобы незамедлительно связаться со своим банком. Виновный достает наряду с конвертом карту с помощью подручных средств. В дальнейшем виновный вводит заранее подсмотренный ПИН-код и снимает деньги со счёта карты [11, С. 325–328].

Объективная сторона мошенничества с использованием электронных средств платежа в современной редакции описана лаконично. Она выражается в действии и характеризуется специальным способом – использованием при мошенничестве электронных средств платежа. В ранее действовавшей редакции способ такого мошенничества был более конкретизирован: использование поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации. На сегодняшний день ситуация не изменилась: и хотя законодатель «не раскрыл» диспозицию нормы, способ указанного деяния остается прежним. Если совершение деяния не предусматривает участие уполномоченного работника кредитной, торговой или иной организации при совершении деяния содеянное квалифицируется как п. «г» ч. 3 ст. 158 УК РФ (с банковского счета, а равно в отношении электронных денежных средств (при отсутствии признаков преступления, предусмотренного статьей 159.3 УК РФ). Указанный пункт был введен тем же Федеральным законом, что и новая редакция ст. 159.3 УК РФ [2].

Следовательно, полагаем, что в рамках исследуемого состава преступления также одним из обязательных признаков выступает обман в специфической форме путем предоставления уполномоченному работнику организации или иному лицу – заведомо ложных сведений в отношении прав на электронное средство платежа (в том числе платежную карту).

В соответствии с положением п. 2 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» обман как способ совершения хищения или приобретения права на чужое имущество может состоять в сознательном сообщении (представлении) заведомо ложных, не соответствующих действительности сведений, либо в умолчании об истинных фактах, либо в умышленных действиях, направленных на введение владельца имущества или иного лица в заблуждение [12]. В отношении состава преступления, предусмотренного ст. 159.3 УК РФ, обман заключается в использовании поддельного или принадлежащего другому лицу средства платежа (в том числе платежной карты) для оплаты товара или услуг, выдавая себя за лицо, имеющее законное право распоряжаться денежными средствами данной карты или иного средства платежа, и убеждая уполномоченного работника торговой, кредитной, иной организации в этом посредством подписания кассового чека. Следовательно, законодатель предусмотрел возможность направленности обмана не только на потерпевшего, имеющего право распоряжения имуществом, но и на третьих лиц, которые таким правом не обладают, а выступают лишь в роли лиц, присутствующих при совершении преступления.

Приведем пример. Объективная сторона совершенного деяния выразилась в том, что З., находясь у здания, увидел на тротуаре банковскую карту, оформленную на имя И., решил похитить с данной карты денежные средства путем оплаты различных услуг и товаров. Так, введя продавца-кассира Х. супермаркета в заблуждение относительно своей личности, предъявил эту банковскую карту, будто бы он является лицом имеющим право распоряжаться денежными средствами, содержащимися на банковской карте, расписался в кассовом чеке, подтвердив тем самым законность пользования данной картой, оплатив товары на сумму 18999 руб. 55 коп. [13].

Проблема практического плана прослеживается, если задуматься, мог ли уполномоченный работник противодействовать совершению указанного деяния? Особенно рассуждение актуально, если вспомнить, что ныне терминалы оплаты, установленные в организациях, для совершения операции могут требовать, а могут и вовсе не требовать ввода ПИН-кода. Более того, если незаконный держатель карты вводит ПИН-код, который необходим для совершения операции именно этим устройством, то в данном случае будет ли обман направлен на сотрудника организации? В данном случае механизм расчета и списания денежных средств во многом

идентичен механизму «обналичивания» денежных средств посредством банкомата.

Не лишена логики позиция Р.А. Сабитова и Е.Ю. Сабитовой, которые отмечают, что законодатель «поспешил» принимать статью в подобной редакции (*прим. – авторы научной статьи анализировали первоначальную редакцию рассматриваемой статьи от 29.11.2012*). Они аргументируют свою позицию тем, что, если обман не направлен на потерпевшего, используется как средство облегчения доступа к имуществу, направлен на третьих лиц, значит, такой обман не обусловливает передачу имущества, значит, не воздействует на волю лица, имеющего право распоряжаться данным имуществом, то изъятие имущества происходит тайно или открыто, помимо воли собственника или иного владельца имущества. По их мнению, подобные действия нельзя признать мошенничеством [14, С. 19].

В самом деле, уполномоченный работник той или иной организации не является лицом, которое имеет право распоряжаться денежными средствами, находящимися на лицевом счете держателя карты, а также лицом, которое правомочно принимать решения о списании денежных средств. И вообще такой сотрудник не может ограничить право держателя карты распоряжаться денежными средствами. Когда происходит обман представителя торговой организации (к примеру, официанта), то вряд ли кем-то фактически удостоверяется – является ли лицо правомочным держателем карты или нет. Денежные средства списываются со счета еще до момента получения чека расплачивающимся лицом, который должен поставить на нем свою подпись. Соответственно, обман, используемый виновным, является средством облегчения доступа к имуществу.

Анализ объективной стороны состава мошенничества с использованием электронных средств платежа (в том числе платежных карт) позволяет сделать вывод, что имеет значение, ставится ли подпись в чеке или предъявляется ли паспорт. По замыслу законодателя именно таким образом лицо, оплачивающее товары, услуги, удостоверяет, что именно оно является владельцем данного платежного средства. Вместе с тем на практике достаточно с умыслом на хищение чужого имущества передать, в частности, платежную карту уполномоченному работнику либо вставить ее в соответствующее считывающее устройство, набрать код или выполнить другие действия, направленные на оплату товара или услуг по требованию уполномоченного работника кредитной, торговой или иной организации. Применительно к использованию платежных карт сегодня существуют такие считывающие устройства, которые вовсе не

требуют ввода ПИН-кода, в том числе для этих целей созданы приложения, фиксирующие данные платежной карты, позволяющие оплачивать покупку прикосновением телефона к считывающему устройству. В такой ситуации обмана работника организации в собственном смысле нет.

В этой связи, присутствие уполномоченного работника организации при незаконном изъятии денежных средств при помощи платежной карты не является препятствием для хищения безналичных денежных средств. Представляется, что сотрудник и вовсе не осознает противоправность действий преступника.

Значит, разграничение кражи и мошенничества с использованием электронных средств платежа по признаку присутствия сотрудника торговой, кредитной или иной организации является, конечно, верным, но недостаточным. В свете изменений в УК РФ, в соответствии с которыми средством совершения мошенничества, предусмотренного ст. 159.3 УК РФ, стали не только платежные карты, но и иные электронные платежные средства, подобные рассуждения приобретают еще большую актуальность. Довольно сложно представить в новых условиях участие уполномоченного работника. Однако же видится, что выделение данного состава преступления обусловлено в большей степени именно использованием в процессе совершения деяния средств платежа, а значит, для обмана на сегодняшний день в нынешних законодательных реалиях достаточно простого их предоставления. Можно охарактеризовать умолчание о личности пользователем средства платежа как обман в пассивной форме.

В целом, по нашему мнению, рассматриваемая статья УК РФ, безусловно, отвечает интересам общества и служит защите прав правообладателей электронных средств платежа. Тем не менее, нормы, содержащиеся в данной статье, не проработаны и требуют корректировки. После серьезных изменений в ст.ст. 158 и 159.3 УК РФ назрела необходимость в разъяснениях высшей судебной инстанции по вопросам квалификации указанных смежных составов преступлений.

Полагаем, что для успешной борьбы с рассматриваемым видом мошенничества от государства требуется совершенствование обеспечения безопасности использования электронных средств платежа. В частности, этому будет способствовать отказ от бесконтактной технологии оплаты, которая была разработана в целях уменьшения времени обслуживания покупателя.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954.
2. О внесении изменений в Уголовный кодекс Российской : федерации Федеральный закон от 23.04.2018 г. №111-ФЗ // Российская газета. – 2018. – 25 апреля. – № 7551 (88).
3. Статистика: количество платежных карт, эмитированных кредитными организациями // Центральный банк Российской Федерации [Электронный ресурс]. – Режим доступа: http://www.cbr.ru/statistics/p_sys/print.aspx?file=sheet013.htm – Загл. с экрана. (дата обращения 28.04.2018).
4. Статистические отчеты по форме 10-а за 2014, 2015, 2016, 2017 гг. // Судебный департамент при Верховном Суде [Электронный ресурс]. – Режим доступа: http://www.cdep.ru/ – Загл. с экрана. (дата обращения: 29.01.2018).
5. Дашидондокова, А.Ц. Проблемы безопасности расчетов пластиковыми картами / А.Ц. Дашидондокова, Н.А. Духанина, Е.Н. Смольянинова // Фундаментальные исследования. – № 2. – 2015.
6. О национальной платежной системе : федеральный закон от 27.06.2011 г. № 161-ФЗ // Собрание законодательства РФ. – 2011. – № 27. – Ст. 3872.
7. Кочои, С.М. Ответственность за корыстные преступления против собственности / С.М. Кочои. – М., 2000.
8. Положение об эмиссии платежных карт и об операциях, совершаемых с их использованием: утв. Банком России 24.12.2004 № 266-П (ред. от 14.01.2015) // Вестник Банка России – 2005. – № 17.
9. Харламова, А.А. Проблемные вопросы квалификации мошенничества с использованием платежных карт / А.А. Харламова // Вестник Уральского юридического института МВД России. – 2017. – №1.
10. Павлова, Е.В. Россия и современный мир: ключевые проблемы в экономической сфере / Е.В. Павлова, Т.Е. Снхчян // Молодой ученый. – 2014. – № 4. – С. 589–593.
11. Карева, Е.И. Мошенничество с пластиковыми картами в России / Е.И. Карева // Молодой ученый. – 2015. – № 1.
12. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда РФ от 30.11.2017 г. № 48 // Российская газета. – 2017. – 4 декабря. – № 7446 (280).
13. Приговор Нововятинского районного суда г. Кирова от 13.09.2013 г. № 1-101/2013(41286) [Электронный ресурс]. – Режим

доступа: http://sudact.ru/regular/doc/nwC8TR2VSrxQ/ – Загл. с экрана. (дата обращения: 01.02.2018).

14. Сабитов, Р.А. Уголовно-правовая оценка обманов и действий, совершенных с документами / Р.А. Сабитов. – М.: Юрлитинформ, 2012.

Г.В. Джихвадзе,
магистрант Юридического института
Алтайский государственный университет, г. Барнаул

В.А. Мазуров,
к.ю.н., доцент кафедры уголовного права и криминологии
Алтайский государственный университет, г. Барнаул

ВОПРОСЫ ОПРЕДЕЛЕНИЯ ПРЕСТУПНОСТИ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В ИНФОРМАЦИОННОЙ СЕТИ ИНТЕРНЕТ

В настоящее время, информационная сеть Интернет (далее – Интернет) становится все более массовым средством реализации конституционных прав, благодаря своей доступности и простоте использования. Однако вместе с тем, как писал сербский дипломат и ученый Й. Курбалийя, Всемирная Сеть является своеобразным «зеркалом» реального мира, где отражаются современные социальные и политические процессы, некоторые из которых несут негативный характер [1]. Для современного российского общества и законодателя крайне актуальным является вопрос состояния и противодействия преступности экстремисткой направленности в Интернете.

Актуальность данной темы обусловлена тем, что информационная сеть «Интернет» становится все более массовым средством связи между гражданами по всему миру, благодаря своей доступности и простоте использования. Так, первостепенную роль в такого рода связи играют социальные сети - сайты, предназначенные для общения и связи между пользователями, где может быть размещена информация самых разных видов: мультимедиа, видео- и аудиофайлы, графические изображения. И, как мы уже отмечали, в социальных сетях, как сайтах публичного пользования, так или иначе отражены реальные социальные, политические и духовные вопросы,

которые имеют место быть в реальной жизни. Таким образом, актуальным остается вопрос определения преступности экстремистской направленности в социальных сетях, а также ее профилактике.

Главной целью нашего исследования анализ методов определения и противодействия преступности экстремистской направленности в социальных сетях. Нам необходимо дать правовую характеристику понятию «экстремистская деятельность», осуществить анализ состояния и динамики преступности экстремистской направленности в Российской Федерации, охарактеризовать механизм определения преступности экстремистской направленности в социальных сетях, выявить в нем проблемные моменты и разработать направления противодействия преступности экстремистской направленности, а также социально порицаемого контента в социальных сетях.

Значимость данного исследования заключается в том, что содержащиеся в работе положения могут быть использованы в нормотворческой деятельности, а также в правоприменительной практике субъектов противодействия преступности экстремистской направленности в социальных сетях.

Говоря о правовой характеристике такого явления как экстремизм, следует, в первую очередь, ссылаться на Конституцию, которая определяет общие начала по противодействию деятельности, которую федеральные законы определяют как экстремистскую. Также Конституция, в главе первой, провозглашает основы конституционного строя, насильственное изменение которых попадает под определение экстремизма [2].

Если говорить о правовой дефиниции экстремизма, то здесь необходимо обратиться к Федеральному закону от 25 июля 2002 г. № 114-ФЗ «О противодействии экстремистской деятельности», где который определяет экстремизм как: насильственное изменение основ конституционного строя и нарушение целостности Российской Федерации; публичное оправдание терроризма и иная террористическая деятельность; возбуждение социальной, расовой, национальной или религиозной розни; пропаганда исключительности, превосходства либо неполноценности человека по признаку его социальной, расовой, национальной, религиозной или языковой принадлежности или отношения к религии и др. [3]

Более узко экстремизм определяет Уголовный кодекс, в ст.282, устанавливающей уголовную ответственность за «действия, направленные на возбуждение ненависти либо вражды, а также на

унижение достоинства человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии» [4]. И особую роль в совершении преступлений экстремистской направленности играет Интернет.

По статистике правового портала «Crimestat», за 2017 год по России, в совокупности, было зарегистрировано 1521 преступление экстремистской направленности, из которых 45 в Алтайском крае, и указанная цифра больше на 5%, чем аналогичный показатель за 2016 год. В 2018 году, на 01.10.2018 было зарегистрировано 1056 преступлений экстремистской направленности, в Алтайском крае – 18 преступлений. Таким образом, мы приходим к выводу, что складывается негативная динамика преступлений экстремистской направленности, однако, на наш взгляд, не является в какой-либо степени опасной и оправданной [5].

Граждане обвиняются в возбуждении ненависти, путем размещения на личных страницах социальных сетей изображений с содержанием, как показывает последующая экспертиза, формально являющимся экстремистским. При этом, неоднократно отмечается отсутствие реального серьезного вреда, общественно-опасных последствий, вследствие, во-первых ограниченного доступа к этой информации, во-вторых, отсутствие прямого умысла у обвиняемых, направленного на возбуждение ненависти и вражды к лицам определенной социальной или национальной группы. Указанные критерии являются необходимыми для возбуждения уголовного дела по ст. 282 УК РФ – такова, помимо всех прочих, позиция Верховного суда РФ, который актуализировал разъяснения по делам о преступлениях экстремистской направленности, в связи с возникшими проблемами в правоприменительной практике – были внесены изменения в постановление Пленума Верховного Суда РФ от 28 июня 2011 г. (ред. от 20.09.2018) № 11 «О судебной практике по уголовным делам о преступлениях экстремистской направленности» [6].

Помимо прочего, Верховный суд указал на то, что преступление, предусмотренное статьей 282 УК РФ, совершается только с прямым умыслом и с целью возбудить ненависть либо вражду, а равно унизить достоинство человека либо группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии, принадлежности к какой-либо социальной группе.

Таким образом, мы приходим к выводу, что размещение лицом в сети Интернет, в частности, на своей странице в соцсети или на страницах других пользователей материала, созданного им самим или

другим лицом, может быть квалифицировано по статье 282 УК РФ только в случаях, когда установлено, что это лицо, т.е. разместившее такой материал, осознавало направленность деяния на нарушение основ конституционного строя, а также имело цель возбудить ненависть или вражду либо унизить достоинство человека или группы лиц по признакам пола, расы, национальности, языка, происхождения, отношения к религии либо принадлежности к какой-либо социальной группе.

Данные факты должны устанавливаться на стадии предварительного следствия, либо рассмотрения сообщения о преступлении [7]. Так, должностное лицо, следователь, ведущий производство по соответствующему материалу, должен получить необходимую доказательственную базу, наличие которой позволит дать правовую оценку действиям лиц участников данного материала. Здесь мы подчеркиваем необходимость сугубо тщательного подхода к следствию, который позволит установить, действительно ли имеет место быть состав преступления, предусмотренного ст. 282 УК РФ и, вообще, совершенное преступление экстремистской направленности.

В связи с вышеизложенным мы приходим к следующим выводам:

1. Мы считаем, что вышеописанный контент, формально попадающий под контент экстремистского характера, не является таковым вследствие отсутствия повышенного общественно-опасного воздействия, а также отсутствия умысла на возбуждение ненависти или вражды. В данном вопросе мы опираемся на действительную позицию ВС РФ, а также ссылаясь на своеобразную культуру общения в социальных сетях, что исключает восприятие данной информации как унижающей человеческое достоинство;

2. Вместе с тем, мы обращаем внимание на вред такой информации. И, на наш взгляд, негативное воздействие такого рода контента заключается, в первую очередь, в том, что онповышает правовую и политическую безграмотность, порождает в потребителях этой информации циничное отношение к государству, праву, а также человеку, его правам и свободам, кроме того, негативно воспринимается многими пользователями сети;

3. С учетом имеющегося негативного воздействия данной информации, считаем необходимым разработку и принятие мер профилактики размещения социально порицаемого контента в социальных сетях, в открытом доступе. Данные меры, помимо всего прочего, должны включать повышение правовой культуры молодежи, среди учащихся старших классов средних учебных заведений и

студентов ВУЗов, как наиболее активных пользователей социальных сетей и Интернета в целом.

4. Что касается ответственности за распространение данной информации, то мы считаем, что существующее ныне уголовное воздействие на лиц, совершивших это деяние, противоречит общеправовому принципу гуманизма, а также принципу соразмерности общественно опасных последствий и последующего наказания. Посему, мы отмечаем необходимость строго индивидуализированного и тщательного подхода органов следствия к материалам проверки такого рода деяний и, в целом, к квалификации их как распространения информации, возбуждающих ненависть и вражду.

Список литературы

1. Курбалийя Й. Управление Интернетом: координационный центр национального домена сети Интернет / Й. Курбалийя // – М.: Проспект, 2010. С. 44.

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом поправок, внесенных Законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 г № 6-ФКЗ, от 30 декабря 2008 г № 7-ФКЗ, от 5 февраля 2014 г № 2-ФКЗ, от 21 июля 2014 г № 11-ФКЗ) // Российская газета. – 1993. – 25 декабря; Собрание законодательства РФ. – 2014. – № 31. – Ст. 4398.

2. О противодействии экстремистской деятельности: Федеральный закон от 25.07.2002 № 114-ФЗ (ред. от 23.11.2015) // Собрание законодательства РФ. –2002. – № 30. – Ст. 3031; 2015. – № 48. – Ст. 6680.

3. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 №63-ФЗ (ред. от 23.11.2018) // Собрание законодательства РФ. – 1996. – № 25. – Ст. 2954; 2018. – № 18. – Ст. 2581.

4. Брайко Д.Н. Обзор профилактических методов противодействия идеологии терроризма и экстремизма в образовательной среде / Д.Н. Брайко // Обзор НЦПТИ. – 2018. – № 2. – С. 56-63.

5. О судебной практике по уголовным делам о преступлениях экстремистской направленности: Постановление Пленума Верховного суда РФ от 28 июня 2011 г. № 11 (ред. от 20.09.2018) // Российская газета. – 2011. – 14 июля.

6. Уголовно-процессуальный кодекс Российской Федерации: Федеральный Закон от 18.12.2001 №174 – ФЗ (ред. от 23.11.2018) // Российская газета. – 2001. – 22 декабря; Собрание законодательства РФ. – 2018. – № 18. – Ст. 2569.

Р.Г. Драпезо,
старший преподаватель
Юридический институт, Кемеровский государственный университет, г. Кемерово

ИСХОДНЫЕ СИТУАЦИИ ПО ПРЕСТУПЛЕНИЯМ, СОВЕРШАЕМЫМ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ, И СПОСОБЫ ЛЕГАЛИЗАЦИИ ОПЕРАТИВНО-РОЗЫСКНОЙ ИНФОРМАЦИИ

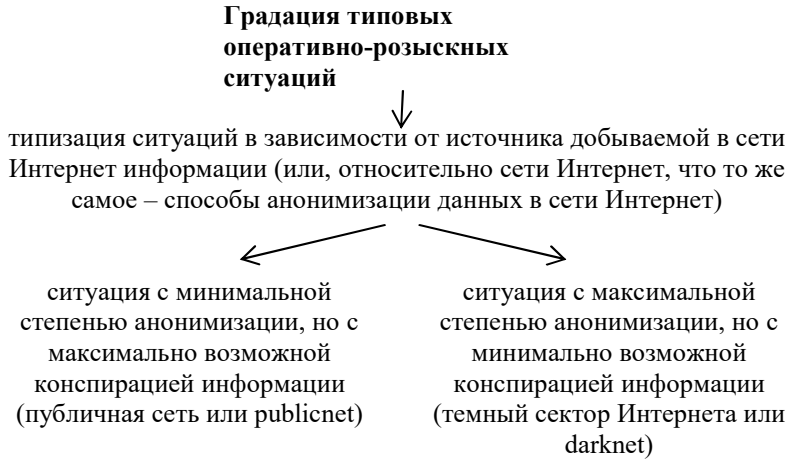
Правоохранительные органы рано или поздно найдут возможности отслеживать правонарушителей в «темном секторе» Интернета («darknet»). Однако появятся новые Интернет-технологии, либо преступники воспользуются уже существующими, но пока не освоенными технологиями, например другими, более безопасными в плане конфиденциального обмена информацией. Можно заблокировать все мессенджеры и ресурсы, по которым идет незаконный сбыт или совершаются другие киберпреступления, включая Facebook, darknet, но проблему это не решит, а усугубит, так как криминал освоит еще более глубокие слои сети Интернета, где отследить их будет практически невозможно. Так произошло с отечественными площадками по незаконному сбыту наркотических средств «Ramp» и «Legal», которые прекратили свое существование, но на смену им пришла еще более мощная интернет-площадка «Hydra» [1].

На наш взгляд, пока наиболее действенными средствами борьбы с киберпреступниками, включая лиц незаконно сбывающими наркотические средства через сеть Интернет, считаются методы, приемы и средства оперативно-розыскной работы и их оперативная комбинация. Для данного высказывания у нас имеются три довода: 1) методы, приемы и средства оперативно-розыскной работы носят универсальный характер вне зависимости от того, что изобретают преступники; 2) комбинирование методов, что создает эффект

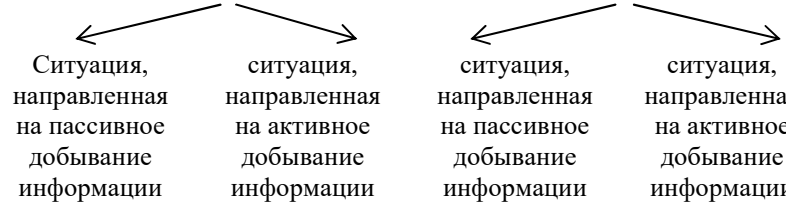
эмерджентности. Другими словами, методы входящие в состав оперативной комбинации или операции, оказываются более эффективными, чем их проведение по отдельности; 3) накопительный эффект, то есть, каждая последующая оперативная информация, каждый последующий негласный агент, позволит более детально отслеживать продавцов и другие промежуточные звенья, устанавливать их личность и место нахождения. Однако для этого, понадобится единая федеральная автоматизированная база данных и математический аппарат, способный устанавливать смысловые корреляции между приведенными выше элементами.

Сказанное потребует решение множества задач, среди которых, для разрешения настоящей статьи, мы выделим такие: 1) изучить особенности добываемой оперативными подразделениями информации в сети Интернет; 2) исходя из ее особенностей, попытаться построить и по мере возможности типизировать исходные оперативно-розыскные ситуации, возникающие при решении задач предупреждения, выявления и раскрытия преступлений, совершаемые с использованием сети Интернет; 3) предложить способы легализации добываемой оперативно-розыскной информации в уголовно-процессуальные доказательства.

Взяв за основу идеи типизации исходных оперативно-розыскных ситуаций предложенные Д.В. Кимом [2] и С.И. Давыдовым [3], на схеме рисунка 1 мы приводим возможную типизацию исходных ситуаций, которые возникают по преступлениям, совершаемые через сеть Интернет.



типизация ситуаций от условия получения значимой для решения задач оперативно-розыскной деятельности информации



типизация ситуаций в зависимости от значимости добываемой информации и использованием для этих целей оперативно-розыскных мероприятий и иных методов оперативной работы

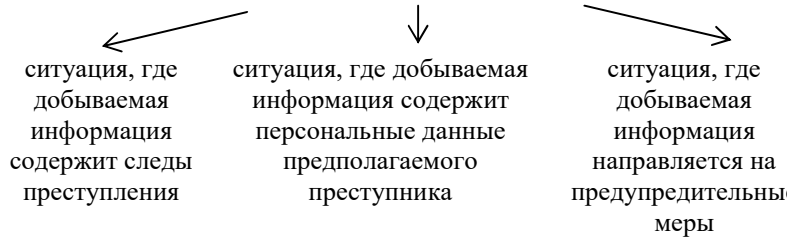


Рис. 1. Типизация исходных оперативно-розыскных ситуаций, которые возникают по преступлениям, совершаемые через сеть Интернет, в зависимости от особенностей добываемой информации.

В основу типизации положены особенности добываемой информации. Из рисунка 1 видно, что в качестве особенностей, выступают: источники и анонимность добываемой в сети Интернет информации, условие ее получения и криминалистическая значимость информации. После того, как будет определено место предполагаемого или совершаемого преступления (публичный либо темный сектор Интернета), далее оперативный сотрудник решает использовать пассивное либо активное добывание информации. Пассивное добывание предполагает мероприятия по поиску, розыску, мониторингу и т.п. в сети Интернет информации, которая может иметь криминалистическое значение. Далее информация фиксируется, легализуется в уголовно-процессуальную информацию и приобщается к материалам уголовного дела в качестве доказательства.

Активное добывание предполагает использование «острых» методов и приемов оперативной работы, которые способствуют

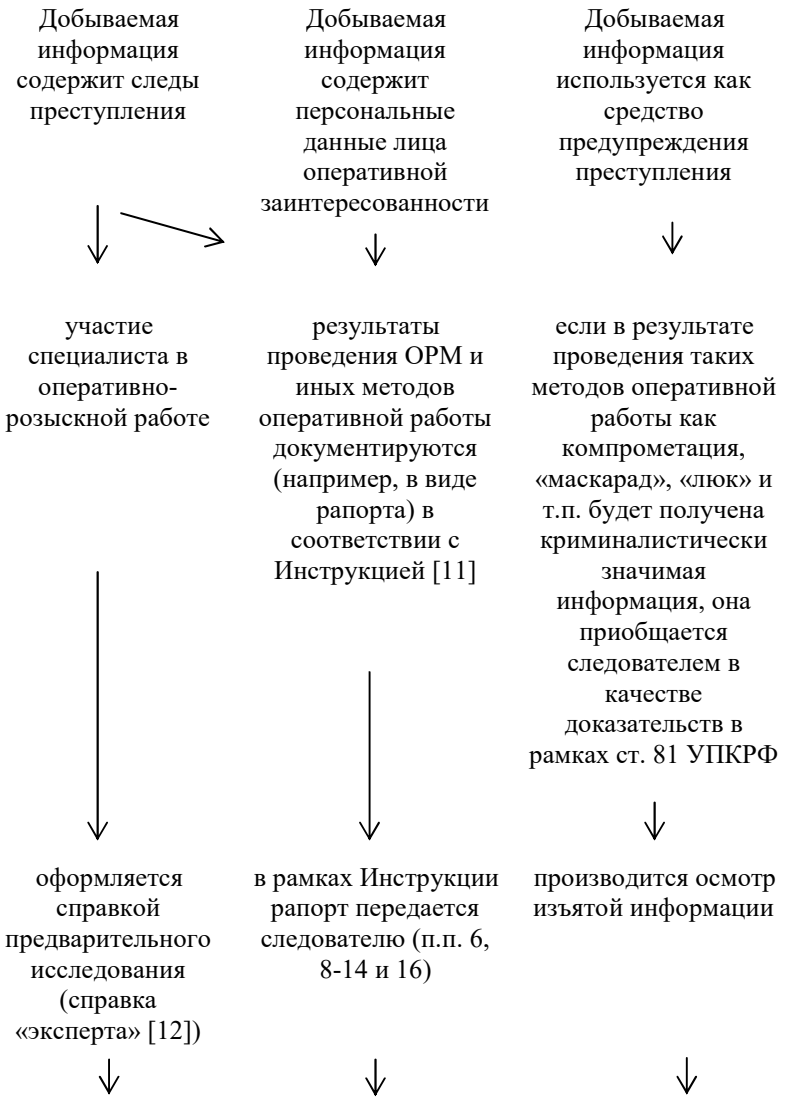
созданию благоприятной оперативной обстановки с тем, чтобы побудить лиц оперативной заинтересованности совершать такие действие, которые выгодны оперативным подразделениям. Например, отказаться от преступного замысла, привлечь некоторых сбытчиков наркотических средств к сотрудничеству в качестве негласных агентов или закрыть интернет-магазин (например, на сетевом ресурсе «Hydra») по незаконному сбыту запрещенных к обороту предметов или веществ, так как последний был скомпрометирован оперативными сотрудниками и т.п. Так, в таблице 1, мы приводим и сравниваем некоторые более или менее оптимальные методы и приемы оперативной работы в публичном и темном секторе Интернета. Можно видеть, что эмерджентность, упомянутая нами в начале статьи, достигается в комбинированном использовании средств и методов оперативной работы. Так, к примеру, фишинг (по отношению к лицам оперативной заинтересованности это выманивание у последних конфиденциальных данных, включая логины и пароли [9]) может быть применен оперативным сотрудником как самостоятельный метод для решения задач выявления и раскрытия преступления, так и в комбинации с компрометацией, для решения профилактических задач.

Таблица 1.Сравнение некоторых приемов и средств оперативно-розыскной работы, проводимые в публичной сети Интернет и сети darknet

Приемы и средства	Особенности приемов и средств	Особенности применения
1. Компрометация	- используя различные оперативно-технические средства, доставить лицу оперативной заинтересованности информацию различной степени достоверности [4] (дезинформация); - дезинформация доставляется либо заподозренному лицу, либо кругу лиц, так или иначе контактирующих с этим лицом; - по своей природе имеет	- компрометация может быть направлена на сам предмет незаконного сбыта через сеть Интернет, на интернет-магазин, либо против лица оперативной заинтересованности (например, продавец); - компрометация в настоящее время носит пока профилактический характер (например, пресечение незаконного сбыта оружия,

	сложную природу, так помимо самого метода компрометации, применяются методы и приемы оперативной работы [5], например, манипуляция, дезинформация, легендирование, создание благоприятной оперативной обстановки [6].	наркотических веществ и т.п.).
2. Методы компьютерной разведки	- фишинг; - «уборка мусора»; - активный перехват; - осмотр cookie; - электромагнитный перехват информации; - «люк»; - отслеживание номеров Qiwi-кошельков; -маскарад [7, 8] и др.	- перехват логинов и паролей, IP-адреса, mac-адреса, персональных данных [9]; - сбор и фиксация статистики посещения Интернет-ресурсов лиц оперативной заинтересованности и т.п.; - так в уголовном деле (№ дела в суде 2-13/2012 и 2-55/2011 [10]) вышли на сбытчиков наркотических средств после разработанной оперативной комбинации, когда оперативные сотрудники через интернет-ресурс определили время и место «закладки». В назначенное время пришло лицо с одной дозой наркотика. Задержанный дал информацию об остальных участниках преступной группы.

Ниже на рисунке 2 мы приводим разные пути легализации добываемой оперативно-розыскной информации в уголовно-процессуальные доказательства в зависимости от ее характера.



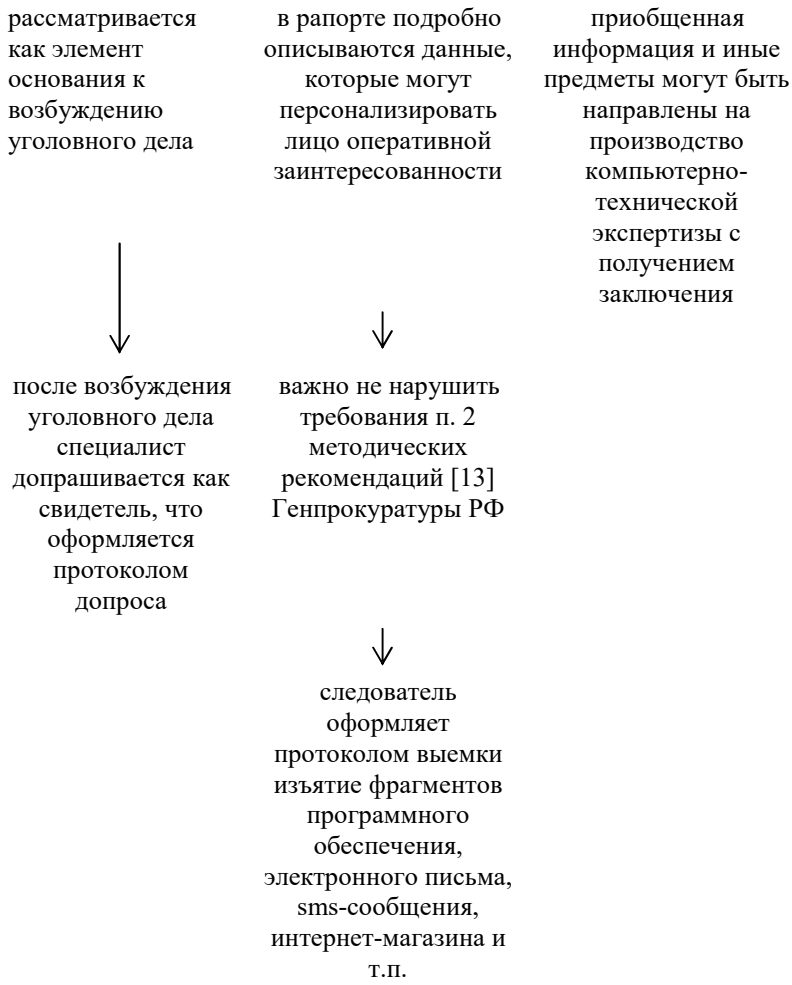


Рис. 2. Способы легализации добываемой оперативно-розыскной информации в уголовно-процессуальные доказательства в зависимости от ее характера.

Видно, что добываемая информация может: 1) послужить основанием для возбуждения уголовного дела; 2) быть приобщена к материалам уголовного дела в качестве доказательств; 3) быть

использована как ориентирующая либо как информация профилактического характера. Кроме того, проанализировав судебную практику, в частности по преступлениям, предусмотренные п. «б» ч. 2 ст. 228.1 УК РФ мы, в отличие от работы А.Г. Волеводза [14], где автор обозначил лишь место собирания доказательств в компьютерных сетях, мы сгруппировали те источники доказательств, на которых суд строит обвинение и выносит обвинительный приговор (рисунок 3).

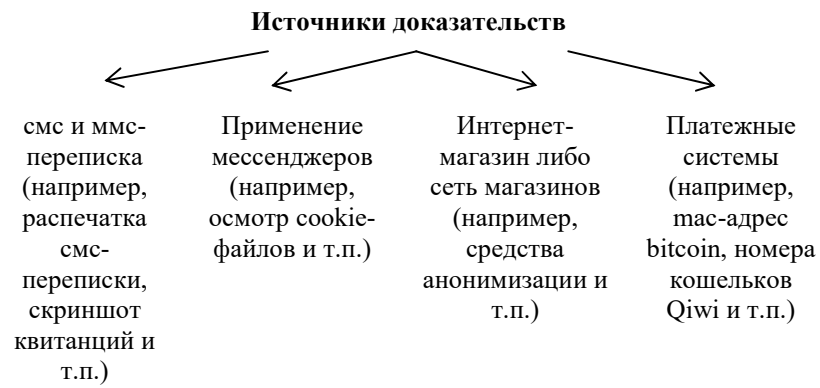


Рис. 3. Часто встречаемые источники доказательств согласно материалам судебной практики по преступлениям, предусмотренные п. «б» ч. 2 ст. 228.1 УК РФ.

Подобные сведения должны быть интересны для оперативных сотрудников, так как тактика оперативной работы последних будет направлена на поиск и фиксацию той информации, которая перспективна для уголовного процесса, с последующей ее легализацией и приобщением в качестве доказательств к материалам уголовного дела.

Таким образом, в зависимости от свойств добываемой в сети Интернет информации выстраиваются исходные оперативно-розыскные ситуации и осуществляется ее легализация для дальнейших целей уголовного процесса.

Список литературы

1. Драпезо Р.Г., Зникин В.К. Darknet как источник сыскной информации / Р.Г. Драпезо // Оперативник (сыщик), - 2017, - Т. 52, № 3. С. 35-38.

2. Ким Д.В. Теоретические и прикладные аспекты криминалистических ситуаций: монография / под ред. проф. В.К. Гавло. - Барнаул: Изд-во Алт. ун-та, 2008. -196 с.

3. Давыдов С.И. О создании базового комплекса рекомендаций по разрешению оперативно-розыскных ситуаций раскрытия преступлений /С.И. Давыдов // Российский следователь. 2010. № 6. С. 32 - 35.

4. Кокурин Г.А. Использование метода компрометации в оперативно-розыскной деятельности // Российский юридический журнал. 2016. № 5. С. 164 - 169.

5. Практика уголовного сыска. Научно-практический сборник: составитель - А. Ваксян. - М.: Лига Разум, 1999. – 244 с.

6. Драпезо Р.Г., Кондратьев М.В. Об актуальности оперативно-розыскной деятельности на современном этапе развития государства // Вестник Кемеровского государственного университета. 2015. № 2-2. С. 170-176.

7. Домарев В.В. Защита информации и безопасность компьютерных сетей. К.: Издательство «ДиаСофт», 1999. 480 с.;

8. Ярочкин В.И. Информационная безопасность: Учебник. М.: Фонд «Мир»: Акад. проект, 2003. - 639 с.

9. Павлюков В.В. Правовые и практические аспекты получения компьютерной информации о киберпреступниках / В.В. Павлюков // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- 118 с. С. 77-86.

10. Архив уголовных дел Кемеровского областного суда.

11. Приказ МВД России № 776, Минобороны России № 703, ФСБ России 3 509, ФСО России № 507, ФТС России № 1820, СВР России 3 42, ФСИН России 3 535, ФСКН России № 398, СК России 3 68 от 27.09.2013 «Об утверждении Инструкции о порядке представления результатов оперативно-розыскной деятельности органу дознания, следователю или в суд».

12. Сердюкова Д.В. Особенности возбуждения уголовного дела и типичные ситуации доследственной проверки по делам о контрафактной продукции // Судебная экспертиза. 2006. № 3. С. 84 - 85.

13. «Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании

преступлений в сфере компьютерной информации» (утв. Генпрокуратурой России) // URL: http://genproc.gov.ru (по состоянию на 06.12.2018).

14. Волеводз А.Г. Следы преступлений, совершенных в компьютерных сетях / А.Г. Волеводз // Российский следователь. 2002. № 1. С. 4 – 12.

В.В. Ерахмилевич,
доцент кафедры уголовного права и криминологии
Алтайский государственный университет, г. Барнаул

Е.П. Суханова,
старший преподаватель кафедры уголовного права и криминологии
Алтайский государственный университет, г. Барнаул

НЕКОТОРЫЕ ОСОБЕННОСТИ ВЫЯВЛЕНИЯ И РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ НЕСОВЕРШЕННОЛЕТНИХ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ СЕТИ ИНТЕРНЕТ

В связи с развитием компьютерных технологий преступления против половой неприкосновенности личности все чаще стали совершаться с использованием сети «Интернет», причем данный вид преступности приобретает международный масштаб. Данные деяния квалифицируются по признакам преступлений, предусмотренных ст. 135 УК РФ - развратные действия без применения насилия лицом, достигшим восемнадцатилетнего возраста, в отношении лица, не достигшего шестнадцатилетнего (ч. 1), либо четырнадцатилетнего возраста (ч. 2). В случае недостижения потерпевшим двенадцатилетнего возраста, подобные действия квалифицируются по п. «б» ч. 4 ст.132 УК РФ-иные действия сексуального характера с использованием беспомощного состояния потерпевшего, совершенного в отношении лица, не достигшего четырнадцатилетнего возраста. На это прямо указывается в приложении к ст. 131 УК РФ, согласно которому, к преступлениям, предусмотренным п. «б» ч. 4 ст.132 УК РФ относятся деяния, подпадающие под признаки преступлений, предусмотренных частями второй-четвертой ст. 135 УК РФ, совершенные в отношении лица, не достигшего

двенадцатилетнего возраста, поскольку такое лицо в силу возраста находится в беспомощном состоянии, то есть не может понимать характер и значение совершаемых с ним действий.

Раскрытие и расследование таких преступлений имеет свои особенности, которые, прежде всего, связаны с установлением виновных лиц. Причем, если личность субъектов преступлений против половой неприкосновенности в целом не отличает высокий уровень образования (согласно исследования, проведенного Н.Ю. Скрипченко - профессором кафедры уголовного права и процесса Северного (Арктического) федерального университета имени М.В. Ломоносова, только 5 % испытуемых имели высшее образование, 15%- средне специальное, 30%- начальное профессиональное, 34%- основное общее, 11% имели образование на уровне 5-7 классов), то среди субъектов аналогичных преступлений совершенных с использованием «Интернет-ресурсов» отмечается высокий уровень образования и интеллекта.

Эти лица, обладая хорошими познаниями в сфере компьютерных технологий, изощренно скрывают свои адресные и анкетные данные, что делает затруднительным установление их электронных данных. Например, субъекты данных преступлений регистрируют свои электронные страницы с использованием сим-карт, зарегистрированных на других лиц.

Проблемой является затрудненный доступ к некоторым интернет ресурсам, которые зарегистрированы на территории других государств (Скайп, ВотсАпп, и т.д.). Установление ip-адресов, привязанных к этим операторам возможно только путем направления международных поручений, которые положительных результатов в выявлении причастных лиц в основном не дают.

В случае если удается изъять у интернет-провайдера информацию о посещении (фактах выхода) в информационно - телекоммуникационную сеть Интернет, с указанием IP-адресов посещаемых сайтов пользователей (подозреваемого, потерпевшего) в интересующее следствием время, существует проблема, что соответствующая информация хранится ограниченное время, в течение примерно 1 месяца.

Важным является изъятие и осмотр всей информации с электронных носителей, в том числе скрытой, удаленной. Эта информация зачастую содержит сведения о других фактах противоправной деятельности подозреваемых, обвиняемых, может служить характеризующим материалом.

В большинстве случаев субъекты подобных преступлений проживают на удаленном расстоянии от потерпевших- в других городах, регионах России и даже в других государствах. Это доставляет определенные проблемы при проведении следственных действий, их сроках, а так же определении подследственности. По сложившейся практике уголовные дела расследуются по месту выявления этих преступлений, как правило, это место жительства потерпевшего.

Следует отметить и высокий уровень латентности данных преступлений. В большинстве случаев факты противоправных действий правоохранительным органам становятся известны от родителей несовершеннолетних. В силу особенностей поведения подростков отмечается их склонность к ведению общения в интернет ресурсах, о котором они не склонны сообщать родственникам. Лица, занимающиеся воспитанием несовершеннолетних, в основном узнают о подобных фактах случайно. Механизмы же выявления таких преступлений специальным органами не выработаны и имеют сложность, которая связана с охраняемой законом неприкосновенностью частной жизни, тайной переписки, телефонных переговоров и иных сообщений.

Особенностью данного вида преступлений можно назвать потерпевшего, который в этом случае специальный, а именно несовершеннолетний. Поэтому таким потерпевшим рекомендовано проведение комплексной комиссионной психолого-психиатрической экспертизы, где среди прочих, необходимо выяснения вопроса о склонности испытуемого ко лжи, фантазированию и т.д.

Допрос несовершеннолетнего потерпевшего по преступлениям против его половой неприкосновенности имеет специфику, которая обусловлена как особым характером совершенного преступления (его сексуальной направленностью), так и личностными особенностями самого допрашиваемого, формирующимися из трех основных составляющих:

- возраст допрашиваемого [1, с.191];
- уровень развития и воспитания [2, с. 83];
- психологические черты, сформированные у допрашиваемого [3, с.133] .

При допросе потерпевшего особое внимание необходимо обратить на выяснение вопроса о том, известно ли было собеседнику о его возрасте, кто явился инициатором противоправных действий и детально уточнить, в чем выразились эти действия.

Особенностью является и необходимость проведения лингвистической судебной экспертизы по интернет-переписке, на разрешение которой рекомендованы следующие примерные вопросы:

- Идет ли речь о половой сфере человека в сообщениях пользователей в переписке?

- Кто является инициатором темы «половая сфера человека»?

-Имеются ли в представленных сообщениях признаки побуждения собеседника к действиям, имеющим отношение к половой сфере, к развратным действиям? Если да, то к каким именно действиям побуждается собеседник? Каков характер волеизъявлений в выраженных побуждениях (просьба, требование, угроза и др.)?

- Содержатся ли в сообщениях лингвистические признаки информации порнографического характера?

Возможно также проведение искусствоведческой судебной экспертизы для выяснения вопроса о том, является ли конкретное изображение порнографическим.

Список литературы

1. Ложкин С.Б. процессуальный порядок досудебного производства по уголовным делам о насильственных действиях сексуального характера с участием несовершеннолетних: дис. … канд. юрид. наук. Ижевск, 2004. С.191

2. Брусенцева В.А. Методика расследования ненасильственных сексуальных преступлений: дис. … канд. юрид. наук. Воронеж, 2005. С.83

3. Милованова М.М. Методика расследования сексуальных преступлений, совершаемых в отношении малолетних детей: дис. … канд. юрид. наук. М., 2003. С.133

И.Г. Иванова,
к.ю.н., доцент кафедры уголовного процесса и криминалистики
Сибирский федеральный университет, г. Красноярск

БОРЬБА С ВЕРБОВКОЙ ТЕРРОРИСТОВ ЧЕРЕЗ СОЦИАЛЬНЫЕ СЕТИ (МЕЖДУНАРОДНО-ПРАВОВОЙ АСПЕКТ)

В настоящее время особую остроту приобрел вопрос вербовки молодых людей в террористические организации через социальные сети. Такие негативные тенденции в Интернете усилились на фоне сирийского кризиса и активизации ИГИЛ (запрещенной в России и во многих странах мира террористической организации). Именно эта организация одной из первых начала вести работу в Интернете по захвату умов будущих террористов, распространению радикального ислама и идеологии терроризма. С развитием социальных сетей, таких, как «Вконтакте», «Одноклассники», «Фейсбук», люди стали выкладывать чересчур много информации о себе в открытый доступ, делиться своими мыслями и переживаниями на просторах интернета с неограниченным кругом лиц. По этим данным можно легко составить психологический портрет человека и найти «слабое звено».

Вербовка – это процесс достаточно длительный и требует индивидуального подхода к каждой жертве. Общая схема вербовки состоит из четырех этапов:

1. Предварительный этап – изучение человека без контакта с ним. Вербовщик выявляет основу для мотивации из личностных качеств, идейных соображений жертвы.
2. Установление близких межличностных отношений. Основная цель этого этапа для вербовщика – психологически сблизиться с объектом вербовки.
3. Вовлечение объекта в выполнение просьб вербовщика.
4. Формулирование вербовочного предложения (путем использования компромата, угроз, предложения материальных благ, идеологической мотивации и т.п.).

Вербовщики хорошо понимают и практически используют психологию людей. Люди, склонные к вербовке, относятся к так называемым группам риска, которые могут быть завербованы в силу своего психологического типа личности, как в тоталитарную секту, так и в террористическую организацию. Ниже приводятся их основные категории.

1) люди, остро переживающие глубокую личностную драму, психическую травму;

2) люди, считающие, что их стремление к духовному развитию осталось не удовлетворенным в жизни;

3) личности, сконцентрированные на оккультизме;

4) люди с комплексом патологического альтруизма;

5) идеалистически настроенные подростки и свободолюбцы, склонные к инфантильному поведению в любом возрасте;

6) люди, не удовлетворенные в социальном признании, не имеющие ценностных ориентиров в своей жизни;

7) люди, которые запутались в причинах неэффективности своих решений, психологически устали от необходимости что-то самим выбирать и не хотят нести ответственность за свой выбор [1, С. 98].

Нашумевшим делом в РФ является история Варвары Карауловой – двадцатилетней студентки МГУ. Она получила загранпаспорт в МИДе и вылетела в Стамбул, где ее задержали с группой россиян, которые также, предположительно, пытались попасть в Сирию. Широкую известность этот случай получил из-за того, что отец Варвары сразу сообщил о случившемся в СМИ, Интерпол, МИД России и Турции. Через некоторое время в Следственном комитете выяснили – девушка вела общение с джихадистами. Ее обвинили по ч.1 ст. 30, ч. 2 ст. 205.5 УК (участие в террористической организации со сроком лишения свободы от пяти до десяти лет).

Еще одним известным случаем вербовки граждан РФ является история московского актера Вадима Дорофеева, который бросил свою семью и отправился воевать в Сирию на стороне ИГ, там он и погиб в декабре 2014 года. Отговорить Вадима от ухода в ИГИЛ пытался самый авторитетный исламский богослов Москвы, но было уже слишком поздно.

Наиболее известным примером вербовки за границей является террористка ИГ «Белая вдова» – британка Салли Джонс. Вся страна узнала ее только в 2015 году как самую разыскиваемую британскую террористку. В рядах исламистов Салли оказалась после того как халифату присягнул ее муж, в дальнейшем она перевезла в Сирию сына. Салли стала лидером женской бригады Аль-Хансаа. В июне 2017 года Салли Джонс и ее сына убил беспилотник США.

Обобщая вышеизложенные примеры, можно сделать следующие практические выводы. В группе риска находятся пользователи социальных сетей от 16 до 35 лет. В процессе вербовки

изучается их мировоззрение, психические особенности и физические недостатки. Вербовке преимущественно подвержен определенный тип – внушаемые, ведомые люди. У таких людей нет своих идей, взглядов, жизненных установок, нередко страдают чувством неполноценности. Данный портрет позволит вести профилактические мероприятия в указанной группе.

Для выявления вербовщиков, установления лиц и группировок, занимающихся террористической и экстремистской деятельностью создаются специальные подразделения в правоохранительных органах. Так, в 2006 году в Великобритании антитеррористический отдел полиции был объединён со специальным служебным отделом лондонской полиции, в результате чего появилась новая организация: 15-я антитеррористическая команда по специальным операциям (Counter Terrorism Command – CTC). Антитеррористическая команда призвана бороться с угрозой терроризма на местном, национальном и международном уровне и поддерживает национальную антитеррористическую сеть [2, С. 48]. В России функцию борьбы с преступлениями в сфере высоких технологий, в том числе и террористической направленности, в системе органов внутренних дел осуществляет Бюро специальных технических мероприятий (БСТМ) МВД России [3, С. 550].

С учетом сложившихся современных тенденций использования террористами социальных сетей для вербовки новых адептов в свои сети, многие страны не только создают специальные подразделения для борьбы с подобными преступлениями, но и на федеральном уровне пытаются усовершенствовать свое уголовное законодательство в сфере противодействия актам террористической вербовки через сеть Интернет и социальные сети.

Сложилось три стратегических подхода, с помощью которых государства противодействуют деятельности террористов в Интернете:

1) принятие законов о киберпреступности общего характера;

2) принятие законов о борьбе с терроризмом (не ориентированных специально на Интернет и социальные сети);

3) принятие специальных законов по борьбе с вербовкой террористов через сеть Интернет.

Так, в Великобритании в части VI Закона о терроризме 2000 года предусмотрен ряд составов преступлений, которые служат основой для предъявления обвинения лицам, использующим Интернет в целях поддержки террористической деятельности.

Статьей 54 этого Закона устанавливается уголовная ответственность за проведение, прохождение или призыв других лиц к

прохождению обучения или инструктажей по изготовлению или использованию огнестрельного оружия, радиоактивных материалов или оружия с их использованием, взрывчатых веществ или химического, биологического или ядерного оружия.

Статьей 57 устанавливается уголовная ответственность за владение соответствующими предметами в обстоятельствах, когда возникает обоснованное подозрение в том, что лицо владеет такими предметами в связи с подготовкой, подстрекательством к совершению или совершением террористического акта. Для того чтобы факт совершения данного преступления был признан, обвинение должно доказать наличие связи между соответствующим предметом и конкретным актом вербовки террористов.

Такое преступление, как подстрекательство к совершению террористических актов, является предметом резолюции 1624 (2005) Совета Безопасности ООН. В этой резолюции Совет призвал все государства, в частности, принять такие меры, которые могут быть необходимы и уместны и будут соответствовать их обязательствам по международному праву, чтобы законодательно запретить подстрекательство к совершению террористического акта или актов и предотвращать такое поведение.

В Великобритании в соответствии со статьей 59 Закона о терроризме 2000 года преступлением считается подстрекательство другого лица к совершению террористического акта полностью или частично за пределами Великобритании, когда такое деяние, будь оно совершено в Англии и Уэльсе, являлось бы одним из преступлений, предусмотренных в данной статье (например, убийство, умышленное нанесение ран, взрывы или создание угрозы жизни в результате повреждения имущества).

В части 1 Закона Великобритании «О терроризме» 2006 года введен ряд новых составов преступлений в целях расширения возможностей принятия органами власти соответствующих мер в случаях, когда те или иные лица выступают с заявлениями, подстрекающими к совершению террористических актов или прославляющими их или иным образом направленными на содействие совершению таких актов.

В Европе статья 3 Рамочного решения 2008/919/ЈНА Совета Европейского союза от ноября 2008 года о внесении поправок в Рамочное решение 2002/475/ЈНА о борьбе с терроризмом и статья 5 Конвенции Совета Европы о предупреждении терроризма обязывают соответствующие государства-члены ввести уголовную ответственность за действия или заявления, представляющие собой

подстрекательство к совершению террористических актов. Конвенция Совета Европы о предупреждении терроризма налагает на государства-члены обязательство криминализовать «публичное подстрекательство к совершению преступлений террористического характера», а также как вербовку, так и подготовку террористов.

В изданном ЮНОДК (UNODC – Управление Организации Объединенных наций по наркотикам и преступности) «Обзоре дел о терроризме» 2010 года анализируются актуальные аспекты международного правового режима противодействия терроризму в таких странах, как Алжир, Египет, Испания и Япония [4].

В Алжире, в соответствии с пунктом 1 статьи 87-bis Уголовного кодекса, совершение террористических актов карается смертной казнью, пожизненным заключением либо лишением свободы на другие длительные сроки. В пункте 4 статьи 87-bis предусматривается, что лица, оправдывающие перечисленные террористические акты, подстрекающие к их совершению или финансирующие их, подлежат наказанию в виде лишения свободы на сроки от 5 до 10 лет, а также штрафа.

В Египте, согласно статье 86-bis Уголовного кодекса, преступлениями считаются деяния, равнозначные ответственности за осуществление и поддержку, планирование и подготовка террористических актов, членство в нелегальных организациях или поддержка таковых, предоставление финансирования и материальной поддержки террористическим организациям, а также подстрекательство к совершению преступлений. Кроме того, данной статьей предусматривается ужесточение наказаний, в частности, за преднамеренное содействие (любыми средствами) достижению целей террористических организаций или за приобретение или производство (прямо или косвенно) предметов, публикаций или записей любого рода, предназначенных для содействия достижению таких целей или их поощрения.

В Японии любое лицо, подстрекающее, прямо или через посредника, к совершению преступления, подлежит такому же наказанию, как если бы данное лицо являлось одним из фактических исполнителей преступления (статья 61 Уголовного кодекса). Другими законоположениями в Японии, такими как статьи 38-40 Закона о предотвращении подрывной деятельности, устанавливается уголовная ответственность за подстрекательство к мятежу или поджогу в целях пропаганды и поддержки какой-либо политической доктрины или политики или противодействия им.

В Испании, в соответствии со статьями 18 и 579 испанского Уголовного кодекса, публичное подстрекательство к совершению преступления, связанного с терроризмом, рассматривается как подготовительный этап преступной провокации. Статьей 578 предусматривается наказание за преступление «восхваление терроризма»; этот состав преступления был введен в Уголовный кодекс Органическим законом № 7/2000 от 22.12.2000 года. Органическим законом также предусматривается наказание в виде поражения в гражданских правах на определенный срок по приговору суда.

В Индонезии не существует норм, специально касающихся деятельности, которую террористы ведут с использованием Интернета, включая подстрекательство к совершению террористических актов. В статье 14 Закона № 15/2003 о пресечении актов терроризма подстрекательство к совершению террористических актов рассматривается без упоминания об использовании преступниками конкретных способов связи, как и в Уголовном кодексе Индонезии, в котором рассматриваются вопросы подстрекательства к совершению других преступных деяний. Компетентные органы Индонезии успешно осуществляют судебное преследование лиц за связанную с терроризмом деятельность в Интернете.

В Сингапуре в контексте использования Интернета подпункт *g* пункта 2 статьи 4 сингапурского Свода правил пользования услугами Интернета запрещает распространение материалов, «восхваляющих этническую, расовую или религиозную ненависть, рознь и нетерпимость, подстрекающих к ним или одобряющим их».

Проанализировав сложившуюся международную практику, приходим к выводу, что страны в большинстве случаев идут по пути криминализации терроризма в Интернете вообще и процесса вербовки в частности, опираясь только на общие уголовно-правовые нормы. На фоне роста террористической угрозы, использования преступниками самых современных средств связи и коммуникации, такой подход представляется не вполне верным. Принятие специальных норм позволит не только давать правильную квалификацию деяниям преступников, совершенных с использованием Интернета и социальных сетей, но и урегулировать проблемные вопросы получения и изъятия цифровых доказательств и последующей их возможности признания судом.

Для эффективного расследования вербовки в террористические организации посредством социальных сетей, вину необходимо подкреплять собранными надлежащим образом и надлежаще

задокументированными доказательствами. Это требуется для установления целостности цифровых доказательств в целях признания их допустимости в суде. К числу ключевых вопросов относятся режим охраны как физического устройства, использовавшегося для хранения или передачи электронных данных, так и самих данных, а также процедуры, примененные для получения этих данных, и любые отклонения от общепринятых методов.

От органов расследования также могут потребоваться доказательства того, что полученная информация достоверно и точно отображает данные, первоначально содержавшиеся на соответствующем носителе, и что они может продемонстрировать связь с ними обвиняемого. Для установления аутентичности можно представлять дополнительные свидетельские показания. Иллюстрацией этой практики может служить дело Адама Басби, который был осужден в 2010 году в Ирландии за отправку в аэропорт Хитроу в Лондоне сообщения об угрозе применения бомбы. Во время суда в дополнение к доказательствам того, что сообщение было отправлено с определенного компьютера, к которому обвиняемый имел доступ, были представлены распечатка журнала регистрации пользования компьютером и телевизионная запись, чтобы установить время, когда было передано сообщение, и доказать, что в это время за компьютером работал именно обвиняемый.

В ряде государств информация из анонимных источников не допускается в качестве доказательства в суде; однако оперативные сведения, подтвержденные авторитетными источниками, могут быть приняты к рассмотрению. Например, в Ирландии собранные разведывательные данные могут считаться достаточно достоверным доказательством того, что лицо является членом незаконной организации, если соответствующие показания дает под присягой сотрудник полиции в ранге не ниже старшего суперинтендента.

Подводя итоги, можно отметить, что для эффективного расследования преступной деятельности, связанной с использованием Интернета и социальных сетей для вербовки террористов, требуется принятие соответствующих законодательных норм, знание доступных инструментальных средств для осуществления незаконной деятельности через Интернет, разработка практических методик получения и исследования цифровых доказательств, а также методических рекомендаций по выявлению и расследованию таких преступлений**.**

Список литературы

1. Соснин В.А. Проблема вербовки людей в террористические секты: социально-психологические факторы / В.А. Соснин // Наука. Культура. Общество. – 2015. – № 4. – С. 94-104.

2. Базаркина Д.Ю. Борьба с терроризмом в Великобритании / Д.Ю. Базаркина // Современная Европа. Журнал Института Совета Европы РАН. – 2015. – № 1. – С. 45-56.

3. Руководство для следователя и дознавателя по расследованию отдельных видов преступлений: в 2 частях. Ч.1 / под ред. Н.Е. Муженской, Г.В. Костылевой. – М.: Проспект, 2013. – 640 с.

4. Обзор дел о терроризме – United Nations Office on Drugs and Crime [Электронный ресурс]. – Режим доступа: https://www.unodc.org/documents/terrorism/Publications/Digest_of

А.Н. Калюжный,
кандидат юридических наук, доцент
Академия ФСО России, г. Орел

ТАКТИЧЕСКИЕ ОСНОВЫ ПРОИЗВОДСТВА ОСМОТРОВ МОБИЛЬНЫХ УСТРОЙСТВ И ДАННЫХ КОНТЕНТА ИНТЕРНЕТ-РЕСУРСОВ ПО ДЕЛАМ О ПОСЯГАТЕЛЬСТВАХ, НАПРАВЛЕННЫХ НА СВОБОДУ ЛИЧНОСТИ

Реалии современной действительности свидетельствуют об увеличении в структуре преступности посягательств, ранее не характерных для общественных отношений, среди которых получили свое распространение преступления, направленные на свободу личности [1]. Похищение человека, его продажа, использование рабского труда и другие посягательства на свободу личности все чаще используются для удовлетворения своих корыстных, низменных интересов, используются как средства получения прибыли, изменения своего социального и семейного статуса [2, С. 210].

Механизм совершения указанных посягательств обуславливает необходимость использования преступниками и потерпевшими телекоммуникационных систем: мобильных устройств, компьютеров, планшетов и ноутбуков, посредством которых фигуранты обмениваются сообщениями и ведут диалоги, подготавливая условия для совершения преступлений. Необходимость рекламирования

завуалированных услуг (продажа в бездетные семьи детей, продажа для занятия проституцией девушек, продажа внутренних органов доноров и т.п.) побуждает виновных подавать такие объявления в социальных сетях «Facebook», «ВКонтакте», «Одноклассники» и других, а также использовать мессенджеры (WhatsApp, Telegram, Viber и др.), вступая в переписку с «покупателями» и «жертвами».

Одним из технических средств, применяемых преступниками по посягательствам на свободу личности, являются мобильные устройства сотовой связи, с помощью которых определяются и согласовываются их преступные действия, координируются действия сообщников по подготовке и сокрытию преступной деятельности, выдвигаются завуалированные предложения будущим «жертвам», уточняется стоимость предлагаемых услуг с «покупателями товара» и т.п.

Современные возможности средств мобильной связи, позволяя осуществлять звонки и обмениваться сообщениями посредством сотовой связи и интернет-технологий, имеют характерную для них специфику механизма следообразования, поскольку образованные ими следы не отображаются во внешней материальной обстановке, нося информационный характер [3, С. 10].

Изобличение преступной деятельности виновных предполагает производство комплекса оперативно-розыскных мероприятий, процессуальных, следственных и иных действий, среди которых наиболее распространенным, на первоначальном этапе расследования указанных преступлений, является осмотр, производство которого допустимо до возбуждения уголовного дела (ч.1 ст.144 УПК РФ).

В число наиболее типичных объектов осмотра предметов по делам о посягательствах на свободу личности входят, изъятые мобильные устройства, являющиеся неотъемлемым атрибутом современного человека, фиксирующим элементы преступной деятельности: отображая данные соединений абонентов, SMS-сообщений, переписку мессенджеров, информацию социальных сетей и др.

Тактические основы осмотра мобильных устройств по делам о посягательствах на свободу личности предполагают внесение в протокол осмотра предметов следующей криминалистически значимой информации:

а) наименование (марка) телефона, его цвет, внешний вид, а также индивидуальные особенности: фон рабочего стола, царапины, повреждения и т.п.;

б) информация, содержащаяся в списке контактов, находящаяся в «журнале звонков» и в «телефонной книге» аппарата. В ходе ее описания обращается внимание на даты и время контактов виновных друг с другом, с потерпевшим, его родственниками, а также «покупателями товара»;

в) данные папки (списка) SMS-сообщений, сделанных за интересующий период абонентом (переписка виновных; угрозы и требования, направленные потерпевшему или родственникам; предложения «покупателям товара»; сообщения о списании или зачислении денежных средств со счетов потерпевшего или родственников на счета виновных и т.п.);

г) данные, содержащиеся в интернет браузерах, осматриваемого телефона (Opera, Яндекс браузер, GoogleChrome и др.), так как они содержат информацию о датах и времени посещаемых сайтах (размещенных рекламных услуг, предложений труда похищенной жертвы, подбираемых орудиях и средствах преступления, подыскиваемого для удержания потерпевшего жилья и др.);

д) данных находящихся в мессенджерах (Telegram, Viber, WhatsApp и др.), а также социальных сетях (Одноклассники, Instagram, Вконтакте и т.п.), посредством которых преступники общались друг с другом, с потерпевшим и предполагаемыми «покупателями». Указанные данные содержат криминалистически значимую информацию, раскрывают содержание переписки, изобличают фотографиями и видео-файлами отдельные элементы преступной деятельности, свидетельствуют о местоположении фигурантов, используемых ими сетях Wi-Fi [4, С. 3]. Кроме того, доказательственное значение имеют данные о местонахождении абонента в их сопоставлении с местом и датами похищения, удержания, эксплуатации потерпевшего;

е) имеющиеся фото и видео-файлы, хранящиеся в «галерее» осматриваемого мобильного устройства.

Получаемые в ходе осмотров мобильных устройств данные являются криминалистически значимыми и служат необходимым средством доказывания преступной деятельности, совершенной преступниками, в отсутствии свидетелей преступных посягательств на свободу личности. Например, в ходе осмотра мобильного устройства подозреваемого Ш. в папке «галерея» была обнаружена видеозапись избиения потерпевшей А., которую последний похитил, удерживая в заранее приготовленном помещении по мотивам ревности [5].

Поскольку, как мы указали ранее, посягательства на свободу личности зачастую совершаются посредством вовлечения

потерпевших и «покупателей» услуг с использованием социальных сетей, возникает необходимость осмотра контента, содержащегося на станицах «Одноклассников», «Facebook» и других. Осмотр контента социальных сетей имеет свои тактические особенности, заключающиеся в описании следующего:

а) через какое устройство осуществлялся доступ в сеть Интернет и каким браузером;

б) на какой сайт зашли и адрес данного электронного ресурса, введенного в диалоговую строку;

в) содержание загрузившейся на сайте социальной сети анкеты пользователя.

Далее отражаются результаты просмотра, особое внимание при котором обращается на описание:

г) списка пользователей, с которыми осуществлялась переписка;

д) содержание просматриваемой переписки, общения, их период и история.

Для подкрепления наглядности осматриваемого контента и исключения возможности последующего удаления переписки выполняются снимки (скриншоты) экрана компьютера или мобильного устройства, с которых был осуществлен доступ к конкретным социальным сетям, веб-адресам. Выполненные действия фиксируются в протоколе осмотра, а сделанные скриншоты веб-страниц приобщаются к протоколу осмотра в качестве приложений.

Несмотря на возможность производства целого ряда осмотров в порядке ч. 1 ст. 144 УПК РФ до возбуждения уголовного дела, полагаем, что осмотр и копирование информации через средства телекоммуникации должно осуществляться по судебному решению или с согласия пользователя (абонента). Например, Воробьев Н. совместно с Михайловой А. вступили в преступный сговор между собой, направленный на торговлю людьми и, посредством переписки в социальной сети «ВКонтакте», обманным путем привлекли потерпевшую в г.Москву, где пытались продать за 500 тыс. рублей. В ходе проведения осмотра контента социальной сети «ВКонтакте» была выявлена и зафиксирована переписка виновных с потерпевшей [8].

В случае необходимости для участия в проводимом следственном действии может привлекаться специалист [6, С. 31] и использоваться специализированная криминалистическая аппаратура [7, С. 98].

Список литературы

1. Состояние преступности в России за январь – декабрь 2017 г. М., 2018.

2. Авдеева Е.В. Преступления против свободы личности в Российской Федерации // Криминологический журнал Байкальского государственного университета экономики и права. 2014. № 2. С. 210-212.

3. Багмет А.М., Скобелин С.Ю. Актуальные вопросы применения криминалистической техники для получения информации, содержащейся в мобильных электронных устройствах // Вестник криминалистики. 2013. № 4 (48). С. 10.

4. Васюков В.Ф., Булыжкин А.В. Некоторые особенности осмотра средств сотовой связи при расследовании уголовных дел // Российский следователь. 2014. № 2. С. 3.

5. Архив Старооскольского районного суда Белгородской области // Уголовное дело № 1-278/2014.

6. Скобелин С.Ю. Использование специальных знаний при работе с электронными следами // Российский следователь. 2014. № 20. С. 31.

7. Рогова И.А., Бурцева Е.В. Практика применения UFED – универсального устройства для криминалистического исследования мобильных устройств // Евразийский союз ученых. 2015. № 7 (16). С. 98.

8. Архив Перовского районного суда г. Москвы // Уголовное дело № 1-09/2016.

А.С. Князьков,
доктор юридических наук, доцент; заведующий кафедрой криминалистики
Томский государственный университет, г. Томск

СЛЕДСТВЕННЫЕ ДЕЙСТВИЯ И ОПЕРАТИВНО-РОЗЫСКНЫЕ МЕРОПРИЯТИЯ КАК СРЕДСТВА ИЗУЧЕНИЯ ЛИЧНОСТИ ПРЕСТУПНИКА ПРИ РАССЛЕДОВАНИИ НЕЗАКОННОГО СБЫТА НАРКОТИЧЕСКИХ СРЕДСТВ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Возрастание объема преступлений, способами которых выступают информационные технологии, в том числе незаконного сбыта наркотических средств путем использования электронных информационно-телекоммуникационных сетей, требует комплексного рассмотрения широкого круга вопросов противодействия отмеченным деяниям, в том числе положений, касающихся их раскрытия и расследования.

Во многом успех борьбы с незаконным оборотом наркотических средств предопределен продуктивностью исследования криминалистической наукой многочисленных аспектов, характеризующих саму преступную деятельность и следственную деятельность, направленную на её познание. Нельзя не сказать о заметных успехах ученых-криминалистов, разрабатывающих алгоритмы поисково-познавательной деятельности при обнаружении признаков совершения преступлений с использованием информационных технологий. Об этом, например, свидетельствуют материалы научно-практических конференций, посвященных отмеченным положениям [1].

Вместе с тем, нельзя не заметить, что новизна и специфический характер механизма преступления, обусловленного задействованием указанного способа, а также своеобразие виртуальных следов, объективно предопределили сосредоточение внимания на преступной деятельности, оставив за рамками научного интереса вопрос о личностных свойствах обвиняемых по преступлениям такого рода. Однако вряд ли достаточным для раскрытия и расследования этих преступлений будет ограничение проблемы изучения личности преступника анализом вопроса о том, какими технологическими знаниями он должен обладать с целью задействования тех или иных программных средств.

Лишь в определенной мере способствуют решению задачи изучения личности преступника, осуществляющего незаконный сбыт наркотических средств путем использования электронных или информационно-телекоммуникационных сетей, публикации, в которых рассматриваются вопросы использования социальных сетей для отыскания и анализа сведений, имеющихся в аккаунте человека, а именно: на «личной страничке», в разделах «Сообщения» и «Документы» [2, с. 5-11]. Оценивая информационную значимость довольно обширных по своим характеристикам таких сведений, нельзя забывать о том, что они появились, по большей части, вне связи с совершением лицом преступления. И по этой причине можно отыскать охотно сообщаемые лицом сведения биографического характера (его фамилия, имя, отчество, год рождения, возраст и социальное положение и т.п.), собственные характеристики (выдающиеся качества, знания, умения и навыки), к которым, в силу некой отстраненности автора от коммуникантов, следует подходить критически. Здесь невольно напрашивается аналогия относительно свободных и экспериментальных образцов, которым справедливо придается разная оценка.

Совсем иначе обстоит дело в тех случаях, когда лицо использует рассматриваемые технологии в качестве средств совершения ряда преступлений, например, неправомерный доступ к компьютерной информации, мошенничество, склонение к совершению самоубийства, развратные действия, незаконный оборот порнографических материалов, организация экстремистского общества и организация деятельности экстремистской организации: распространяемые им сведения о себе являются преимущественно ложными, они выбираются под будущую жертву, в том числе адресуются неопределенному кругу лиц, которые, по мысли преступника, охотно воспримут эти сведения. Столь же неконкретной, к тому же, весьма ограниченной, является размещаемая в Интернете информация о лицах, осуществляющих незаконный сбыт наркотических средств безотносительно выбранного способа их реализации.

Если посмотреть более внимательно на проблему исследования личности субъекта, осуществляющего незаконный сбыт наркотических средств, то можно прийти к выводу о том, что именно работы, посвященные данной совокупности преступлений, содержат наименьший объем криминалистически значимых сведений о личности преступника.

Так, например, в работе О.А. Есиной вместо личностных характеристик дается общая характеристика ролей участников организованных групп, посягающих на установленный порядок оборота наркотических средств [3, с. 60-67].

Еще более сжатой выступает характеристика субъектов, оказывающих противодействие расследованию наркопреступлений: здесь, судя по всему, предполагается, что лишь путем называния таких субъектов (знакомых обвиняемого, его родственников, коррумпированных сотрудников органов внутренних дел, руководителей преступных групп, журналистов) уже осуществляется их личностная характеристика, имеющая значение для раскрытия и расследования преступлений [4, с. 33-57].

В отдельных работах личностная характеристика субъектов, осуществляющих незаконный сбыт наркотических средств, сводится к выяснению организационных связей руководства и подчинения между участниками преступных групп [5, с. 61-83].

Небезынтересным будет анализ произошедших изменений в личностных характеристиках субъектов преступной деятельности в сфере высоких технологий. В отдельных работах отмечается, что «…на смену старым преступникам в сфере высоких технологий приходят новые. Но этим новым хэкерам уже совершенно не обязательно превосходно разбираться в компьютерах…» [6, с. 56].

Также констатируется, что произошли заметные изменения в психологических чертах личности названной категории преступников: на смену стеснительности, замкнутости и скрытности приходят открытость и коммуникабельность [6, с. 58]. Применительно к личности преступников, осуществляющий незаконный сбыт наркотических средств путем использования электронных информационно-телекоммуникационных сетей, исходя из проанализированного нами значительного объема уголовных дел, можно согласиться с указанным утверждением.

Учитывая это, следует говорить об некоторых положениях, касающихся изучения личности устанавливаемого преступника, подозреваемого и обвиняемого в совершении данных преступлений при выполнении оперативно-розыскных мероприятий и следственных действий. При этом нужно исходить из того, что специфика изобличения лиц, осуществляющих незаконный сбыт наркотиков рассматриваемым способом, проявляется, как верно отмечается в специальной литературе, в исключительно важной роли оперативно-розыскных мероприятий [7, с. 118-120].

Однако нельзя не заметить, что в ходе производства оперативно-розыскных мероприятий задача изучения личности преступника сотрудниками органа, осуществляющего оперативно-розыскную деятельность, решается в наименьшей мере. Так, например, в справках по результатам оперативно-розыскного мероприятия «наблюдение» совершенно отсутствуют сведения о поведенческих реакциях наблюдаемого лица, хотя подчас оно контролировалось длительное время.

Одной из возможностей доказывания причастности определенного лица к незаконному сбыту наркотических средств путем использования информационных технологий является тщательный анализ результатов оперативно-розыскных мероприятий с целью поиска отобразившихся личностных особенностей. Так, в случае отказа задержанного лица от факта использования им сотового телефона, с которого осуществлялись необходимые для совершения сбыта наркотика сообщения, может быть назначена автороведческая экспертиза. Её результативность предопределена тем, что при выполнении смс-сообщений наблюдается устойчивое проявление таких факторов, как выбор шрифта для сообщения, написания цифр, прежде всего времени, использование знаков препинания и т.д. В качестве примера приведем следующую смс-переписку участников преступной группы:

134579 2014-06-11 15:03:22 Входящее Я ДОБАВЛЮ

134580 2014-06-11 15:03:36 Входящее БУДЕТ РОВНО

134581 2014-06-11 15:05:38 Исходящее Хорошо

134582 2014-06-11 15:05:45 Исходящее По 0,4 да да

134583 2014-06-11 15:05:53 Исходящее только 0,4

134585 2014-06-11 15:08:20 Входящее ДЕНЮЖКУ НАДО

134586 2014-06-11 15:09:13 Исходящее Да кину

О некоторых личностных качествах обвиняемого может говорить используемый им логин. Так, например, Сед-н Р.И. был зарегистрирован в социальной сети Xabber под логином «tankist@exploit.im» «NIKNAIM» «Tankist». Такого рода сведения должны использоваться для установления и поддержания психологического контакта с обвиняемым, склонения его к даче правдивых показаний и в целом – к сотрудничеству со следствием.

В определенной мере об уровне развития лица, осуществляющего незаконный сбыт наркотических средств путем

использования информационных технологий, могут свидетельствовать изъятые блокноты, тетради и отдельные листы с рукописными записями о местах оставления наркотических средств, об учете наркотических средств и преступно полученных денежных средств и их расходовании, а также своего рода «маршрутный лист» закладчика наркотиков в определенных местах. Такого рода листы выполняются с целью передачи сведений о местах закладки так называемому «диспетчеру», осуществляющему связь с приобретателями наркотика.

В практике расследования встречаются случаи, когда при задержании лица, осуществляющее рассматриваемую преступную деятельность, у него обнаруживаются огнестрельное оружие, а также «заявление» о том, оно случайно обнаружило это оружие. Такого рода заявления пишутся заранее и имеют целью убедить следствие и суд в случайном обнаружении этого оружия лицом непосредственно перед его задержанием и в намерении сдать его в полицию. Текст подобного «заявления» тоже может использоваться для выявления личностных характеристик подозреваемого (обвиняемого), а в некоторых случаях – и для производства судебной почерковедческой экспертизы.

Анализ материалов уголовных дел по незаконному сбыту наркотических средств путем использования информационных технологий позволяет указать на характерную ошибку при производстве допроса подозреваемых, обвиняемых и свидетелей. Она состоит в отсутствии тактической задачи выявления личностных характеристик членов преступной группы: все вопросы о личности ограничиваются вопросами об употреблении лицом наркотических средств.

Крайне редко выявляются сведения о личностных свойствах субъекта в его повседневных отношениях с другими лицами, например, членами семьи, в том числе с детьми. Важность таких сведений возрастает в тех случаях, когда члены семьи, например, муж и жена (сожитель и сожительница) являются членами преступной группы, осуществляющей незаконный сбыт наркотических средств рассматриваемым способом. Так, например, в материалах одного уголовного дела имеется расписка П-ды, данная своему сожителю в том, что она обязуется употреблять наркотики в меньших количествах. Невыполнение такого обещания приводило к её избиению сожителем, выбрасыванию её сожителем из движущегося автомобиля, к иным действиям, демонстрировавшим превосходство сожителя.

По данной категории уголовных дел весьма редко проводятся судебно-психологические экспертизы с целью изучения личностных свойств подозреваемых (обвиняемых). Имеющиеся в дела судебно-

психологические экспертизы направлены на выяснение преступной роли, которую выполнял в организованной группе тот или иной её участник.

Примером может служить следующий вывод эксперта: «Типовыми предметами побуждения источником исходящих сообщений (лицом «М») источника входящих сообщений (лица «Ж») являются: получить (взять) материал для работы, найдя его по указанному адресу (описанию места); расфасовать (взвешивая, раскладывать на части определенного веса, упаковывать) полученный (найденный) материал; разместить (спрятав) расфасованные и упакованные предметы (сделать «клады») в различных местах в городе, с учетом инструкций относительно того, где, как, когда прятать; сообщить адреса сделанных «кладов», по запросу уточнить адреса (описание мест) сделанных «кладов». Типовыми предметами побуждения лицом «Ж» лица «М» являются принять адреса сделанных «кладов»; дать работу; выдать зарплату; а также инструктирование, как найти спрятанный «клад». В тексте проанализированного общения имеются также речевые указания на следующие функции собеседников: лицо «Ж» занимается торговлей в розницу; к компетенции лица «М» относится изменение статуса лица «Ж» до оптового продавца; лицо «М» является работодателем по отношению к лицу «Ж»; роль лица «Ж» обозначена словом «курьер»; лицо «М» предоставляет лицу «Ж» сведения о месте нахождения материала для работы, получив предварительно эти сведения от субъекта, обозначенного словом «опт»; лицо «М» осуществляет торговлю через собственный магазин».

В заключение необходимо сказать, что имеющийся в настоящее время опыт выявления лиц, осуществляющих незаконный сбыт наркотических средств путем использования информационных технологий, позволяет перейти в полной мере к решению задачи изучения личности преступника как предпосылки успешного раскрытия и расследования названных преступлений.

Список литературы

1. Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействия киберпрступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами: сб. науч. ст. /отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул: Изд-во Алт. ун-та, 2017. 118с.

2. Алексеева Т.А., Ахмедшин Р.Л., Юань В.Л. Основные подходы к содержанию криминалистического анализа личности в

социальных сетях // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействия киберпрступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами: сб. науч. ст. / отв. ред. С.И. Давыдов, В.В. Поляков. Барнаул: Изд-во Алт. ун-та, 2017. С. 5-11.

3. Есина О.А. Особенности расследования преступлений, связанных с незаконным оборотом наркотических средств: дис. …канд. юрид. наук. Уфа, 2004. 162с.

4. Петрунина А.Б. Противодействие расследованию преступлений в сфере незаконного оборота наркотиков и криминалистические методы его выявления и преодоления: дис. …канд. юрид. наук. М., 2006. 249с.

5. Шапошников А.Ю. Криминалистическая характеристика преступных групп, действующих в сфере незаконного оборота наркотических средств: дис. …канд. юрид. наук. Саратов, 2001. 285с.

6. Рогозин В.Ю. Изменения в криминалистических характеристиках преступников в сфере высоких технологий // Расследование преступлений: проблемы и пути их решения: сб. ст. М.: Московская академия Следственного комитета Российской Федерации. С. 56-58.

7. Подольный Н.А. Отдельные проблемы расследования преступлений, совершенных с применением компьютерных технологий // Библиотека криминалиста. 2013. № 5. С. 116-127.

И.М. Комаров,
доктор юридических наук, профессор кафедры криминалистики
Московский государственный университет имени М.В. Ломоносова

НЕСКОЛЬКО ТЕЗИСОВ О КРИПТОВАЛЮТЕ

Концепция системы биткойн (децентрализованная система одноименной криптовалюты) была опубликована в ноябре 2008 года её автором (возможно, коллективом авторов) под псевдонимом Сатоси Накамото.

Взрыв популярности биткойна произошел лишь в последние годы. В начале августа 2017 года криптовалюта разделилась на классический биткойн и BitcoinCash. Виртуальные деньги (биткойн) представляют собой всего лишь один из немногих вариантов использования технологии BlockChain (блокчейн), потому, что ещё нет ни одного факта кражи биткойнов и это обстоятельство позволяет говорить о возможной непогрешимой репутации блокчейна во многих важных областях жизни человека, столь же критичных в вопросах безопасности, как денежный оборот (хранение информации, проведение честных выборов и пр.).

Блокчейн – это всего лишь просто распределённая и хорошо защищённая база данных, она схожа с технологией BitTorrent. В первую очередь распределенной структурой и популярностью, но у неё есть и целый рад других достоинств. Система устроена так, что все незаконные попытки внесения изменений в базу, которая основана на технологии блокчейн («похитить» блоки, то есть приписать их себе или добавить новые блоки) всегда пресекаются пользователями посредствам сравнения с копиями хранимых у них баз. Взломать систему также практически невозможно по двум причинам: её децентрализации и многократного копирования хранимой пользователями информации. Это можно сравнить с организацией ДНК в клетках человека. Их много, и они несут в себе всю полноту информации, а при возникновении сбоев легко справляются с ними в отдельных копиях.

В системе электронных денег нет персональных кошельков, то есть отсутствуют данные доступные только владельцу кошелька (участника системы). Имеется один кошелек, однако вся информация о нем открыта для всех участников системы, что означает – статистика всех межличностных расчетов прозрачна. Вмешаться в расчеты двух участников системы (изменить порядок и характер расчетов, совершить хищение и т.п.) третий её участник не может ни при каких

обстоятельствах, по причине того, что так система устроена. Участник системы, между тем, всегда может получить только ему одному предназначенный расчет, он «привязан» к определенным адресам, между которыми и осуществляется транзакция. Получение расчета подтверждается (подписывается) ключом совместимым с адресом (по существу это логин и пароль), а данные о проведении расчета пересылаются по всем копиям базы. Транзакция считается завершенной по окончании сверки записи об отправке и получении расчета.

Что из себя представляет криптовалюта? По идее разработчиков криптовалюта – это «золото» виртуального мира. Количество этого «золота» ограничено расчетами перспективы использования. Однако криптовалюту можно «добывать». Предлагаются три пути добычи: приобретением в «обменнике», на «бирже», либо путем непосредственной «добычи» любым пользователем сети, при условии наличия у него соответствующего оборудования.

Использование BlockChain исключает необходимость привлечения «третьей стороны» (накладные расходы, сроки и пр.) при совершении экономических операций, так как система прозрачна для всех. Кроме того, это свойство (прозрачность) делает её защищенной и безопасной для действий сторон в условиях риска мошеннических действий и необходимости сохранения информации.

Вместе с тем, эти процессы сталкиваются с рядом проблем.

Так, для поддержания высокого уровня безопасности система постоянно нуждается в сложных вычислениях, что возможно только на основе высокой ресурсной базе. Для биткойнов разработчики эту проблему решили просто. Пользователям, которые связаны с «добычей» биткойнов назначают комиссию с тем, чтобы они предоставили свой ресурс, то есть подтвердили возможность майнинга (способ заработка биткойна).

Кроме того, для безопасности системы важно, чтобы ресурсная база была распределена, а не находилась под управлением группы, которая может использовать ресурсы для различных манипуляций.

Криптовалюта не обеспечена никакими экономическими факторами (золото, уровень ВВП) поэтому её курс может легко обваливаться до полного нуля. Этот и другие экономические недостатки вызывают к ней недоверие правительств многих государств. Вместе с тем, в отдельных государствах имеются экономические учреждения, интернет-магазины или сервисы, которые принимают биткойны в качестве оплаты за товары и услуги.

В качестве выводов можно отразить преимущества и недостатки криптовалюты в отношении реально существующих валют.

Привлекательным является независимость системы, её абсолютная защищенность от различных внешних воздействий. При этом прозрачность отношений с криптовалютой доступна каждому пользователю, но влиять на эти отношения он никак не может.

Наличный объем биткойнов всегда ограничен, тиражировать (напечатать) по чьему-то желанию эту валюту невозможно. Её «добыча» сложна с позиции технического подхода. Известны расчеты, которые свидетельствуют, что жизнеспособность криптовалюты обеспечена определенным алгоритмом и «добыть» возможно не более 21 млн. биткойнов. После этого «добыча» не возможна. Сейчас нельзя прогнозировать последствия этого факта, но можно с уверенностью сказать, что при всех благоприятных обстоятельствах криптовалюта останется в обращении с периодическим изменением курса.

Тема технологии BlockChain и криптовалют, на наш взгляд, находится ещё в начале пути, ей нет ещё и десяти лет, между тем криминалистика должна располагать основами соответствующих знаний для того, чтобы быть готовой в нужный момент «вмешаться» в определенные процессы, где могут усматриваться нарушения действующего законодательства и потребуется установить следы нарушений для принятия решения о возможном криминальном характере события.

Подобные проблемы уже возникают в связи с не персонифицированным характером майнинга получения криптовалюты. Этот достаточно широкий круг субъектов как физических, так и юридических лиц фактически получают средства для совершения различных финансовых операций и при определенных обстоятельствах могут быть вовлечены в противоправную деятельность различной направленности (легализация доходов, полученных преступным путем, финансирование терроризма и экстремистской деятельности и т.п.). Криптовалюты могут быть использованы в качестве расчетного средства за результаты противоправной деятельности.

Представляется актуальным уже в настоящее время разрабатывать криминалистические рекомендации относительно отдельных следственных действий, где предметом получения доказательства могут выступать объекты, связанные в криптовалютой. Например, поскольку для пользования биткойнами требуется создание персонального кошелька на основе использования специального программного обеспечения, то важным для процесса производства

обыска обосновать криминалистические действия специалиста как участника обыска связанные с отысканием в компьютере подозреваемого наличия записей с длинными последовательностями символов, ярлыки специализированных программ, сведения о посещении специальных интернет-сайтов для управления электронными кошельками. Эти же действия требуют криминалистического комментирования и для назначения соответствующих судебных компьютерно-технических экспертиз.

Такие рекомендации относительно определенных следственных действий позволят следователю на основе установленного номер электронного кошелька системы Биткойн получить полную информацию об истории операций, балансе, списке и сумме транзакций, номерах кошельков на которые эти средства были отправлены, либо с которых они поступили.

Можно и далее приводить абстрактные примеры тактических криминалистических возможностей доказывания использования преступниками криптовалюты в качестве средства платежа за различные криминальные услуги. Однако это мало повлияет на уже вероятно формирующуюся криминальную ситуацию, где указанные валюты планируются как средства соответствующего платежа. Криминалистам необходимо обратиться к этим вопросам уже «вчера» и на основе данных криминалистической тактики с участием соответствующих профильных специалистов разрабатывать и совершенствовать необходимые рекомендации следственной деятельности.

А.А. Кузнецов,
кандидат юридических наук, профессор, профессор кафедры криминалистики
Омская академия МВД России, г. Омск

С.В. Пропастин,
кандидат юридических наук, доцент,
адвокат Омской коллегии адвокатов «Бизнес и право», г. Омск

А.Б. Соколов,
кандидат юридических наук, доцент кафедры криминалистики
Омская академия МВД России, г. Омск

ПРОВЕДЕНИЕ ОБЫСКА С ЦЕЛЬЮ ОБНАРУЖЕНИЯ И ИЗЪЯТИЯ ЭЛЕКТРОННЫХ НОСИТЕЛЕЙ И ИНФОРМАЦИИ НА НИХ

Электронные носители представляют интерес в качестве источника криминалистической информации. Они могут содержать как сведения о работе компьютера, так и переписку подозреваемого, различные финансовые документы либо видео материалы. Среди следственных действий, наиболее часто проводимых с целью обнаружения таких носителей является осмотр и обыск. В то же время, когда речь идет о поисковых действиях, с целью обнаружения доказательственной информации, наиболее результативным следственным действием является обыск. Процессуальный порядок его проведения регламентирован УПК РФ, а ожидаемые результаты зависят от тактических приемов проведения обыска. Вид и содержание элементов подготовки обыска [3, с. 303 - 308] может варьироваться в зависимости от совершенного преступления. Действия следователя на этапе подготовки к обыску при расследовании преступлений, где объектом выступают электронные носители нами рассматривались ранее [4]. Предполагается, что готовность следователя к проведению обыска не только обеспечивается подготовкой к нему, но и постоянным анализом своих действий во время проведения следственного действия. Говоря о рабочем этапе обыска, следует помнить основные условия успешного его проведения. Это активность и последовательность действий. Под активностью в таких случаях обычно предполагают комплекс мероприятий, обеспечивающих проведение обыска. Однако запланированные действия (проникновение на объект, выбор методов поиска) могут измениться в

зависимости от обстановки, где будет проходить обыск. Поэтому следователь должен находиться в постоянной готовности изменить план действия. Моделирование возможной ситуации, тактический риск – это и многое другое находится в прямой зависимости от действий руководителя следственно-оперативной группы и полученных результатов [2, 5].

Вместе с тем укажем на отдельные особенности, связанные с поддержанием активности следователя во время проведения обыска с целью обнаружения и изъятия электронных носителей и информации на них:

- организационно - тактические усилия следователя (расстановка участников поиска, координация действий поисковых групп и др.);
- своевременное реагирование на любые изменения в поведении присутствующих при обыске лиц (например, попытки выключения электроэнергии, передвижения обыскиваемых, отвлечения внимания участников следственно-оперативной группы громкими выкриками, уничтожения документов и т.п.);
- при возникновении проблемной ситуации изменение тактических приемов обыска, применение мер безопасности для участников следственного действия, а также способов сохранения доказательственной информации;
- обсуждение со специалистом хода и направлений обследования объектов (выбор места начала поиска, определение приемов (методов) поиска, фиксация отдельных действий специалиста посредством фото или видеосъемки и т.п.).

Последовательность действий следователя, как условие проведения обыска, предполагает, что действия поисковой группы будут проводиться по строго условленной схеме: от заранее оговоренных приемов поиска, обнаружения, изъятия объектов до надлежащих способов фиксации хода и результатов обыска. Отклонение от предложенной схемы действий может привести к потере интересующих следствие информации.

Рабочий этап обыска можно подразделить на обзорную и детальную (поисковую) стадии. Обзорная стадия обыска включает обход территории, определение вероятных мест сокрытия искомого и многое другое в основном, связанное с соблюдение процессуальных правил производства данного следственного действия [1, с. 89-126]. Исходя из опыта следственной практики с целью обнаружения и изъятия электронных носителей и информации на них можно также рекомендовать:

1) Уточнение цели, задач и доведение их до участвующих в поисковых действиях сотрудников и специалистов;

2) следователь определяет, какие объекты будет обследовать лично, а какие следует поручить обследовать специалистам, участвующим в проведении обыска. Обращается внимание на наличие помимо самого ЭВМ внешних устройств удаленного доступа;

3) определение и отключение специальных средств защиты информации и средств компьютерной техники от несанкционированного доступа;

4) обнаружение возможной связи между средствами компьютерной техники и каналами электросвязи;

5) фиксирование компьютерной техники, которая находится во включенном состоянии, определение запущенных и исполняемых операционной системой программ и характер проводимых операций. Произвести фотографирование изображения на экране монитора. С помощью специалиста остановить работу исполняемых программ зафиксировав в протоколе данные действия и реакцию ЭВМ;

6) принять меры к созданию надлежащих условий для поиска электронных носителей информации (освещение, определение места, где будет проводиться детальное обследование объектов и т.п.).

На детальной стадии производства обыска с целью обнаружения и изъятия электронных носителей и информации на них действия следователя и иных участников СОГ зависят от методов (тактических приемов) поиска искомого. Наиболее типичными являются:

- по объему обыскиваемых объектов поиск может быть **последовательным** и **выборочным** (в последнем случае обследованию подлежат наиболее вероятные места нахождения искомого);

- в помещении тактически грамотно организовать поиск от направления движения поисковых групп: **встречный** и **параллельный** (например, проведение поиска в различных кабинетах). Параллельный поиск целесообразно проводить в ситуации, когда обыск проводится в помещении, в котором находятся несколько персональных компьютеров и серверный компьютер. Здесь одна поисковая группа может обыскивать отдельно стоящие ЭВМ, другая поисковая группа – серверный компьютер;

- в зависимости от нарушения целостности объекта обыск может быть проведен **с нарушением** его **целостности** или без такового. В ситуации, когда представляется целесообразным изъять внутренний жесткий диск, а системный блок имеет защиту от несанкционированного доступа (замок на крышке системного блока и

др.), следует отыскать ключ от данного замка. В случае, если отыскать ключ от замка крышки системного блока не удалось, а пользователь (собственник) данного персонального компьютера отказывается его открыть, то в целях изъятия жесткого диска следует нарушить целостность замка. Когда же требуется обследование имеющейся информации на жестком диске, нет необходимости в нарушении целостности объекта.

В качестве тактического приема можно рекомендовать согласованные действия следователя со специалистом, когда для обнаружения электронных носителей информации следователь берет на себя организационно-тактическую сторону, а специалист - техническую. Взаимная информация об обнаруженных объектах позволяет определить направления поиска, выявить наиболее удачные тактические приемы, способствующие этому, а также указывает на возможные способы сокрытия информации, применяемые лицом у которых проводится обыск. Следователь, как руководитель следственного действия, принимает решение, где ему находиться во время обыска. Он может вместе со специалистом анализировать информацию, обнаруженную в компьютере или переходя из помещения в помещение контролировать его ход и давать указания о дальнейших действиях. Следует подчеркнуть, что все действия, а также обнаруженные объекты следователь должен доводить до сведения понятых. Данным участникам следственного действия должны быть разъяснены способы изъятия информации с электронных носителей, а также последовательность фиксации в протоколе обыска. Если при этом применялось фотографирование или видеозапись дополнительно следует разъяснять условия их применения. Указанная последовательность должна соблюдаться в обязательном порядке, т.к. к электронным носителям доказательственной информации предъявляются особые требования ввиду их специфических свойств: их невозможно потрогать, осязать, подобные доказательства могут быть подвергнуты изменениям, для их оценки требуются специальные познания. Данное обстоятельство подчеркивает необходимость привлечения понятых, которые должны обладать некоторым объемом знаний в области компьютерных технологий, чтобы понимать суть происходящего события.

В криминалистической литературе отмечается, что для отыскания мест нахождения объектов, в том числе замаскированных, следователь применяет различные тактические приемы, такие как «наблюдение за поведением лица у которого проводится обыск»,

«сравнение однородных объектов», «поиск с применением специальных приборов» и другие.

Наблюдение за поведением лица у которого проводится обыск, а также за реакцией присутствующих заинтересованных участников (родственников, сотрудников) позволяет определить нужное направление поиска. Так, например, определив место, где предполагается сокрытие искомого объекта следователь, приближаясь или наоборот, удаляясь от него, скрытно ведет наблюдение за реакцией обыскиваемого. Уловить реакцию обыскиваемого можно предложив ему определить участок (место) с которого следует начать поиск для обнаружения электронных носителей. Подобные психологические приемы обыска целесообразно использовать при установлении надлежавшего психологического контакта с лицом у которого проводится обыск. При этом обязательным условием достижения результата можно назвать ведение постоянной беседы с ним о расположении помещений, их предназначении, наличии соответствующих ЭВМ и используемых в работе программ.

При обнаружении признаков противодействия расследованию во время проведения обыска следует уделять внимание поиску тайников, мест хранения объектов, замаскированных под иные нужды. Так, сравнение однородных объектов позволяет установить их изменения, не свойственные стандартным характеристикам (при этом учитывается различный вес, внутренний объем, внешний вид поверхности объектов и другие признаки). Это могут быть скрытые ниши стен, размещенные в одной комнате. Их измерения помогут выявить тайник, где вполне может быть размещен сервер. Такой тактический прием целесообразно применять при обследовании внутренней части системного блока, сравнивая обыскиваемый системный блок и стандартный, описанный в технической или справочной литературе. При обнаружении подобных тайников обращается внимание на сходные места, где возможно обнаружение электронных носителей информации.

Что касается проведения обыска с применением специальных приборов то следует предупредить участвующих в следственном действии специалистов (особенно это относится к специалистам-криминалистам, приглашенным для поиска и обнаружения тайников) о том, что нельзя использовать поисковую и досмотровую технику, в основе которой имеется источник электромагнитных или магнитных излучений. Обычно при этом используют инструментальные методы или различного вида оптические зонды.

Если помещений, где проводится обыск много, то целесообразно для учета и контроля за своими действиями подготовить схему расположения объектов, где отразить последовательность их обследования и сведения о сотрудниках, кем именно проводился поиск. В последующем при анализе полученных данных по окончанию обыска такой документ позволит оценить результативность следственного действия и определить последовательность дальнейших следственных действий и оперативно-розыскных мероприятий. Такой документ является рабочим и его приобщение к протоколу обыска не требуется.

Фиксация обыска. Фиксация факта, хода, содержания и результатов обыска с целью обнаружения и изъятия электронных носителей и информации на них, производится по общим правилам, установленным уголовно-процессуальным законодательством.

В любом случае составляется протокол с соблюдением требований, изложенных в статье 166 УПК РФ. В протоколе фиксируются сведения об объектах, обнаруженных и изъятых в ходе обыска (электронные носители, документы, связанные с перепиской интересующих следствие лиц, объекты с традиционными следами, известными в криминалистике (почерк, следы рук и т.п.).

В протоколе обыска, в отличие от протокола осмотра, отсутствует обязательность фиксации подробных сведений об изъятом объекте, так как в дальнейшем можно будет восполнить эти данные путем проведения осмотра предметов и документов. Вместе с тем необходимо фиксировать носитель и их конфигурацию на месте обнаружения, а также упаковку, обеспечивающую правильное и точное соединение в лабораторных условиях [6, с. 213]. В остальном обнаруженные и изъятые объекты описываются по правилам, обозначенным для осмотра.

Дополнительно можно составить схему обнаружения искомых (изъятых) объектов и приложить фотоснимки, в том числе сделанные с применением специальных сканирующих программ. При этом отсутствует необходимость в детальном вычерчивании всего места обыска (схем расположения средств компьютерной техники, каналов и средств связи, инженерно-технических коммуникаций и т.д.).

В завершении отметим, что обыск с целью обнаружения и изъятия электронных носителей и информации на них, проводится с учетом положений УПК РФ и общих криминалистических рекомендаций (активность, последовательность и т.д.). Вместе с тем, имеются особенности реализации таких рекомендаций, в частности применения тактических приемов (например, нецелесообразность

применения раздельного приема поиска; недопустимость использования технических средств, одним из элементов которой является источник электромагнитных или магнитных излучений).

Список литературы

1. Бакиров А.А. Уголовно-процессуальные аспекты производства обыска и выемки: монография / под науч. ред. докт. юрид. наук, проф. З.Д. Еникеева. – М.: Юрлитинформ, 2012. – 192 с.

2. Вражнов А.С. Криминалистический риск при расследовании неправомерного доступа к компьютерной информации: монография. – М.: Юрлитинформ, 2014. – 208 с.

3. Криминалистическая тактика: учебник / под общ. ред. заместителя Председателя Следственного комитета Российской Федерации, руководителя Главного военного следственного управления, кандидата юридических наук, генерал-полковника юстиции А.С. Сорочкина. – М.: Юрлитинформ, 2013. – 728 с.

4. Кузнецов А.А., Пропастин С.В., Соколов А.Б. Обыск как средство отыскания, обнаружения и изъятия электронных носителей и информации на них (подготовительный этап) // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV. С. 59-71

5. Степанов В.В., Бабакова М.А. Поисково-познавательная деятельность при расследовании преступлений, совершенных с использованием высоких технологий: монография. – М.: Юрлитинформ, 2014. – 256 с.

6. Электронные носители информации в криминалистике: монография / под ред. докт. юрид. наук О.С. Кучина. – М.: Юрлитинформ, 2017. – 304 с.

Ю.А. Ложкин,
преподаватель кафедры уголовного процесса и криминалистики
Пермский институт ФСИН России, г. Пермь

ПРОБЛЕМНЫЕ ВОПРОСЫ СОБИРАНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ ПРИ ПРОИЗВОДСТВЕ СЛЕДСТВЕННЫХ ДЕЙСТВИЙ В РАМКАХ ПРЕДВАРИТЕЛЬНОГО РАССЛЕДОВАНИЯ УГОЛОВНЫХ ДЕЛ

В современном обществе происходит непрерывный процесс совершенствования средств передачи информации, разрабатываются и внедряются новые технические устройства для ее обработки и хранения. Стремительное развитие науки и техники неизбежно ведет к стремлению урегулировать с правовой точки зрения те отношения, которые возникают в данной сфере. Между тем, в отечественной правовой науке информационное пространство определяют через единство двух его компонент: техническую, которая включает в себя инфраструктуру связи и коммуникации и социальную – сообщество интернет-пользователей [1]. В связи с этим, нормативное регулирование данной сферы обосновано вызывает объективные сложности. Развитие сети Интернет увеличивает количество внетерриториальных образований и ставит под сомнение основные положения международного права, в частности, традиционное понятие территориальной юрисдикции. Сеть Интернет и другие телекоммуникационные сети образуют кибернетическое пространство, которое является новой человеческой и технологической средой. Пространство не имеет границ, следовательно, не находится под юрисдикцией какого-либо одного государства [2].

Использование злоумышленниками в качестве инструментов совершения преступления сеть Интернет в целом, и различного рода электронные данные, в частности, влечет за собой необходимость принятия со стороны правоохранительных органов мер, направленных на пресечение и раскрытие данной категории преступлений.

Развитие науки и техники привело к появлению нового вида доказательств – электронных доказательств. Они могут быть отнесены к таким закрепленным в Уголовно-процессуальном кодексе РФ, принятым 18.12.2001 Федеральным законом № 173-ФЗ (далее – УПК РФ) доказательствам, как вещественные доказательства и иные документы. Статья 84 данного кодекса предусматривает, что документы могут содержать сведения, зафиксированные как в письменном, так и в ином виде. К ним могут относиться материалы

фото- и киносъемки, аудио- и видеозаписи и иные носители информации, полученные, истребованные или представленные в порядке, установленном ст. 86 УПК РФ. Вещественными такие доказательства могут быть признаны в силу ч. 4 ст. 84 УПК РФ, если они обладают признаками, указанными в ч. 1 ст. 81 УПК РФ. В настоящее время существует немало исследований, посвященных собиранию, проверке и оценке компьютерных или электронных доказательств [3].

Данный вид доказательств является разновидностью доказательств в целом, обладая при этом определенной спецификой, которая заключается в первую очередь в носителе электронных доказательств. Электронные доказательства содержатся на особых носителях: магнитных дисках, серверах, флеш-картах и др. Н.А. Зигура также обоснованно указывает на электронно-цифровую форму представления электронных доказательств [4]. Кроме того, для прочтения (просмотра, прослушивания) электронных доказательств необходимы специальные устройства (компьютер, CD-привод и др.), а также специальное программное обеспечение, позволяющее воспроизвести электронную информацию в том виде, в котором она может быть воспринята человеком. Зачастую трудно установить, является ли тот или иной электронный документ подлинником или копией. Для электронных доказательств характерна также возможность их мгновенного перемещения на большие расстояния. Электронный документ, так же как и традиционный, может быть объектом подлога, причем этот подлог может быть как моральным, так и материальным.

Рассмотрим, как эти особенности отражаются на собирании электронных доказательств. Электронная информация может быть относимой к делу точно так же, как и любые другие непроцессуальные данные. Следовательно, она свободно может использоваться в качестве ориентирующей, тактической информации. Однако для того, чтобы служить доказательством по уголовному делу, фактические данные должны обрести еще и свойство допустимости. Они должны быть получены: 1) надлежащим субъектом доказывания, 2) надлежащим способом собирания доказательств и 3) из надлежащего источника доказательств [5]. Собирание электронных доказательств, как и других видов доказательств, осуществляется путем проведения следственных и иных процессуальных действий. Здесь особо следует выделить обыск, выемку и осмотр. Обнаружение в данном случае возможно путем выявления носителей электронной информации, круг которых может быть чрезвычайно велик. В первую очередь это могут

быть различного рода персональные компьютеры, ноутбуки, планшетные компьютеры, мобильные телефоны, фото-, видеокамеры, мобильные регистраторы, с помощью которых производится фиксация и обработка электронной информации. Кроме того, отдельного внимания при проведении следственных действий, должны заслуживать магнитные накопители информации, функционирующие как внутри электронного устройства (жесткие магнитные диски, внутренняя память телефона), так и предназначенные для переноса информации с одного устройства на другое (флеш-карты, съемные жесткие диски, CD-диски, DVD-диски и т.д.).

Фиксация осуществляется путем изъятия носителя информации с последующим осмотром. Так, например, Гагаринский районный суд г. Москвы в приговоре от 10 июня 2013 г. признал гражданина Т. виновным в совершении преступлений, предусмотренных ч. 1 ст. 183, ч. 2 ст. 183 УК РФ. Суд обосновал виновность указанного лица, в частности, следующими доказательствами: протоколом выемки, согласно которому в ООО «Мэйл.ру» была изъята распечатка сообщений электронной почты, принадлежащей Т., и CD-диск с электронным содержанием сообщений электронной почты; протоколом осмотра, согласно которому были осмотрены предметы и документы, изъятые в ходе проведения выемки в ООО «Мэйл.ру» [6].

Сложнее дело обстоит с обнаружением информации, хранящейся на материальном носителе, находящемся на значительном удалении от места производства предварительного расследования или судебного разбирательства либо в случае иных препятствий к изъятию, например, интернет-сайта или базы данных организации. Первый физически может существовать за пределами Российской Федерации, поэтому изъять и приобщить к материалам дела носитель данной информации довольно сложно. База данных организации зачастую достаточно объемна и защищена от несанкционированного доступа, поэтому при работе с такими доказательствами, как правило, достаточным бывает их осмотр.

Так, одним из доказательств вины в совершении преступления, предусмотренного ч. 3 ст. 138 УК РФ, по делу, рассмотренному мировым судьей судебного участка 9 по Кировскому району г. Уфы Республики Башкортостан, стал протокол осмотра интернет-сайта http://www.ufanic.ru от 7 мая 2010 г. Согласно данному протоколу гражданин А. в присутствии понятых и условного покупателя посетил интернет-ресурс http://www.ufanic.ru. В ходе посещения установлено, что на главной странице сайта имеется вкладка «Оформить заказ». При перемещении по вкладке появляются данные об отсутствии каких-

либо заказов. При выборе в «Каталоге товаров» позиции «Шпионские устройства» отображаются текстовая информация об устройстве «GSM аудиопередатчик (шпион)», фотография устройства, его цена. Данный заказ был направлен в «корзину». В процессе осмотра условный покупатель оформил на вышеуказанном сайте заказ на приобретение GSM аудиопередатчик (шпион) [7].

Еще одним примером может являться приговор Вахитовского районного суда г. Казани от 6 мая 2014 г., в соответствии с которым гражданин Б. признан виновным в совершении преступления, предусмотренного ч. 3 ст. 30, ч. 3 ст. 234 УК РФ. По данному уголовному делу судом было установлено, что гражданин Б. в ходе переписки в одной из социальных сетей с гражданином В., являющимся сотрудником УФСКН России, договорился о сбыте последнему сильнодействующего вещества. Впоследствии Б. сбыл указанное вещество сотруднику УФСКН России, участвующему в ОРМ «проверочная закупка», и был задержан. Письменным доказательством по делу послужил протокол осмотра документов и скриншотов страниц социальной сети, в которых имелась переписка указанных лиц и обговаривались условия продажи сильнодействующего вещества [8].

В этой связи следует отметить большие возможности компьютерной экспертизы для установления обстоятельств, подлежащих доказыванию. Эксперт может ответить на вопросы о наличии тех или иных документов на электронном носителе, дате их создания, изменении и удалении, ведении переписки, отправлении и принятии различных сообщений, аудио-, фотодокументов и видеозаписей.

Кроме того, лицо, осуществляющее расследование уголовного дела, зачастую пользуется таким способом получения доказательств, как ответ уполномоченного органа по результатам мониторинга базы данных. Например, по уголовному делу, рассмотренному мировым судьей судебного участка № 18 Костромского района Костромской области, по обвинению Ч. в подделке водительского удостоверения, одним из доказательств его вины был ответ на запрос из УГИБДД УМВД России по Костромской области, согласно которому по данным компьютерного учета ЦАФАП ГИБДД УМВД России по Костромской области и ФИС «ГИБДД», по состоянию на февраль 2012 г., Ч. водительского удостоверения не имеет. По данным АИПС «Розыск» и ФИС «ГИБДД», бланк водительского удостоверения № 735058 в экзаменационные подразделения ГИБДД РФ не распределялся, водительское удостоверение с таким номером не выдавалось [9].

Рассматривая данное доказательство, следует отметить, что его допустимость и достоверность могут быть поставлены под сомнение. Это доказательство относится к категории последующих, опосредованных. Соответственно, возможно искажение содержащейся в нем информации.

Зачастую с ходатайством о приобщении к материалам дела и последующем исследовании электронных доказательств обращается сторона защиты. Вместе с тем адвокату наиболее часто отказывают в приобщении к материалам уголовного дела таких документов, как распечатка электронных писем, неудостоверенные факсимильные сообщения, документы, размещенные в Интернете, анонимные письма, фотографии [10]. Говоря о критериях допустимости электронных доказательств, можно выделить несколько их видов. Во-первых, общие, которые присущи всем доказательствам. Например, составление протокола, собирание их специально уполномоченным лицом, указанным в законе, участие определенных лиц (понятые, специалист) и т. д. Во-вторых, специальные, присущие только электронным доказательствам. Так, компьютерная экспертиза должна проводиться компетентным специалистом, осмотр сайта должен проводиться следователем, дознавателем, сотрудником органа дознания с участием специалиста и понятых, ход и результаты следственного действия должны быть зафиксированы в соответствующем протоколе и др. В этом смысле к электронным доказательствам должны предъявляться более жесткие требования, поскольку электронные доказательства неосязаемы, для их оценки нужны специальные устройства, а зачастую и лица, обладающие специальными познаниями. Кроме того, электронные доказательства легко могут быть подвергнуты изменениям и уничтожены. Поэтому своевременная и правильная фиксация здесь особенно важна. Это определяет следующие особенности собирания электронных доказательств: оперативность собирания электронных доказательств; участие в собирании компетентного лица; наличие специальных устройств и программного обеспечения, необходимых для собирания доказательств (компьютер, телефон и др.).

Все это находит свое отражение в соответствующих положениях УИК РФ, регламентирующих процедуру получения электронной информации и ее носителей в ходе проведения следственных действий. В частности, изменениями, вносимыми в ст. 182 УПК РФ (основания и порядок производства обыска) и ст. 183 УПК РФ (основания и порядок производства выемки), при производстве рассматриваемых следственных действий, если они

сопряжены с изъятием электронных носителей информации, является обязательным участие специалиста, т.е. лица, обладающего специальными знаниями в рассматриваемой сфере, а также опытом и навыками их применения на практике. При этом, ч. 9.1 ст. 182 УПК РФ и ч. 3.1 ст. 183 УПК РФ не содержит никаких оговорок и исключений, что при буквальном толковании предполагает привлечение специалиста при изъятии любого электронного носителя информации (например, карты памяти, извлеченной из фотоаппарата, отдельно хранящихся флеш-карт или магнитных дисков) по преступлениям всех категорий, что априори затрудняет ход следствия, возлагая на субъекта доказывания совершение дополнительных процессуальных действий, требующих больших временных затрат [11]. Помимо этого, указанные дополнения УПК РФ привели к формированию неоднозначной позиции судов, оценивающих данные доказательства с точки зрения их относимости и допустимости.

Так, Приморский краевой суд признал необоснованным довод апелляционной жалобы об отсутствии участия специалиста при изъятии в ходе обыска электронных носителей информации: ноутбука, USB флеш-накопителя и переносного жесткого диска, поскольку изъятие информации или ее копирование с устройств, не производилось [12]. Данной позиции при принятии решения придерживался Горно-Алтайский городской суд, указав в своем постановлении, что «…при изъятии электронных носителей информации без участия специалиста, копирование информации, содержащейся на изъятых предметах, на другие электронные носители не производилось и сторонами не заявлялось, изъятие ноутбука и внешнего съемного диска не требовало специальных познаний в сфере компьютерной техники, в связи с чем следователем обоснованно принято решение о проведении обыска в отсутствии специалиста» [13]. Еще одним примером может служить решение Судебной коллегии по уголовным делам Оренбургского областного суда, рассматривавшего апелляционную жалобу осужденного Я., который просил отменить приговор, среди прочего ссылаясь на то, что изъятие у него мобильного телефона, являющегося электронным носителем информации, было произведено сотрудниками Линейного отдела МВД России на транспорте без участия специалиста в нарушение ч. 3.1. ст. 183 УПК РФ. Суд признал указанный довод гр. Я. необоснованным, указав, что из смысла ч. 3.1. ст. 183 УПК РФ участие специалиста при производстве выемки в ходе изъятия электронных носителей информации требуется при наличии нуждаемости в данном специалисте, то есть когда необходимо применить специальные

познания и навыки. В частности, если при производстве выемки производится копирование информации на другие электронные носители информации, участие специалиста обязательно, так как это связано с риском утраты или изменения информации. При этом из материалов дела следовало, что при выемке следователь пользовался обычными функциями просмотра телефона, не прибегая к необходимости поиска и открытия закрытых для общего доступа файлов, что говорит о законности произведенных действий [14].

В другом случае, суд пришел к выводу о том, что действия сотрудников полиции в ходе проведения обыска в части изъятия электронной почты (электронных писем), принадлежащей заявителю, системных блоков без соответствующего решения суда и без привлечения специалиста, являются незаконными [15].

Проведенный анализ судебной практики позволяет прийти к выводу, что суды придерживаются позиции, в соответствии с которой, если при проведении обыска или выемки не производилось копирование информации, изъятие каких-либо отдельных деталей электронных носителей (например, жесткого диска из системного блока персонального компьютера), либо изъятие не представляет сложности и не требует специальных знаний и навыков, то привлечение специалиста не является обязательным. Во всех остальных случаях, привлечение специалиста является необходимым. Этот вывод основывается на том, что для обнаружения, фиксации, изъятия системного блока компьютера, ноутбука или карты памяти в их конструктивной целостности при проведении внешнего осмотра следователю достаточно общих криминалистических знаний [16].

Рассмотрев особенности собирания такого вида вещественных доказательств как электронные носители, необходимо сделать основные выводы. Электронная информация сама по себе неосязаема, овеществлен лишь ее материальный носитель, который в дальнейшем и становится вещественным доказательством. В то же время его определение в действующем законодательстве отсутствует, что приводит к неоднозначному пониманию его смысла для субъектов предварительного расследования. Специфика электронного носителя информации как особого вида вещественных доказательств, проявляется в сложности его внутреннего строения как технологичного электронного устройства, обладающего только ему присущими особенностями, и требующая, для должного процессуального закрепления, в некоторых случаях привлечения лица, обладающего специальными знаниями. Вне зависимости от разновидности, электронные носители информации могут выступать в

роли вещественных доказательств, содержащих (хранящих) в себе информацию, имеющую отношение к уголовному делу.

Подводя итог, следует отметить, что использование электронных доказательств в уголовном судопроизводстве является перспективным направлением раскрытия и расследования уголовных дел. Появляются все более и более современные способы, как подтверждения вины лиц, так и ее опровержения. К таким способам следует отнести использование сведений из социальных сетей, переписки по электронной почте, мессенджеров (ICQ, Skype, Viber, WhatsApp и др.). Любая серьезная организация имеет электронный документооборот, существуют различные базы данных государственных и негосударственных организаций. При этом все чаще наблюдается отказ от той или иной части документооборота на бумажном носителе. Можно сказать, что существует постоянное «соревнование» правонарушителей и правоохранителей. Первые используют все более и более совершенные технологии для совершения преступлений и сокрытия следов их совершения, вторые совершенствуют способы раскрытия и борьбы с ними.

При таких обстоятельствах отмечается рост использования компьютерных технологий при совершении преступлений. Преступления все чаще совершаются в отношении компьютерной информации и с использованием компьютерной информации. Для единообразия судебной практики необходим ряд разъяснений высших судебных инстанций по вопросам применения электронных доказательств. Вместе с тем мы считаем, что на данном этапе в изменении закрепленной в УПК РФ системы доказательств, с включением в нее электронных доказательств, нет необходимости. Представляется, что это запутает систему доказательств, ведь электронные доказательства зачастую могут иметь признаки и вещественных доказательств, и иных документов. Кроме того, достаточно сложно в настоящий момент точно определить, какое доказательство является электронным, а какое нет, ввиду их большого объема, разнообразия и постоянного развития. Тем не менее, без правильной, обдуманной работы с такими доказательствами невозможно представить грамотного специалиста, работающего в сфере уголовного судопроизводства ни со стороны обвинения, ни со стороны защиты.

Помимо этого, мы считаем необходимым внесение соответствующих изменений в положения УПК РФ, регламентирующих процедуру изъятия электронных носителей в ходе обыска или выемки, исходя из сложившейся судебной практики.

Существующая в настоящий момент императивная конструкция норм, закрепленных в ч. 9.1 ст. 182 УПК РФ и ч. 3.1 ст. 183 УПК РФ, предписывает привлекать специалистов при любых действиях, связанных с изъятием электронных носителей информации, что не всегда является оправданным и целесообразным. Кроме того, это порождает дополнительные возможность обжалования стороной защиты, законности действий следователя при проведении обыска или выемки электронных носителей информации.

Список литературы

1. Чернышов В.Н., Лоскутова Е.С. Проблемы собирания и использования цифровых доказательств // Социально-экономические явления и процессы. 2017. Т. 12. № 5. С. 199.
2. Искевич И.С., Кочеткова М.Н. Особенности определения места преступления при нарушении авторских прав в глобальном информационном пространстве: международно-правовой и уголовно-правовой аспекты // ППД. 2017. № 1. С. 55.
3. Ефремов И.А. О достоверности электронных документов при осуществлении уголовного судопроизводства // Информационное право. 2006. № 2. С. 21.
4. Зигура Н.А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. ... канд. юрид. наук. Челябинск, 2010.
5. Калиновский К.Б., Маркелова Т.Ю. Доказательственное значение «электронной» информации в российском уголовном процессе // Российский следователь. 2001. № 6. С. 18.
6. Кукарникова Т.Э. Электронный документ в уголовном процессе и криминалистике: дис. ... канд. юрид. наук. Воронеж, 2003.
7. Мухудинова Н.Р. Процессуальная деятельность защитника по собиранию и представлению доказательств в российском уголовном судопроизводстве: монография. Саранск, 2008. С. 28.
8. Архив Вахитовского районного суда г. Казани. Уголовное дело № 1-184/2014. [Электронный ресурс]. URL: http://sudact.ru/regular/doc/WyavwZ7DR958/ (дата обращения: 20 сентября 2018 г.).
9. Полякова Т.А. Вопросы создания правовых условий внедрения электронного документооборота и использования электронных документов в качестве доказательств // Человек: преступление и наказание. 2008. № 1. С. 26.
10. Тульская О.В. Некоторые проблемы использования электронных документов в качестве доказательств в уголовном

судопроизводстве // Вестник Академии Генеральной прокуратуры Российской Федерации. М., 2009. № 6 (14). С. 77.

11. Поплюева К.А. Собирание «электронных» доказательств: некоторые проблемные аспекты // International scientific review of the problems of law. Collection of scientific articles II International correspondence scientific specialized conference. 2018. С. 55.

12. Апелляционное постановление Приморского краевого суда от 24.09.2015 № 22К-5674/2015 [Электронный ресурс]. URL: http://sudact.ru/regular/doc/WyavwZ7DR958/ (дата обращения: 20 сентября 2018 г.).

13. Постановление Горно-Алтайского городского суда Республики Алтай от 10.11.2015 № 3/10- 27/2015 2015 [Электронный ресурс]. URL: http://docs.pravo.ru/document/view/ 79864212/91500342/ (дата обращения: 20 сентября 2018 г.).

14. Апелляционное определение Судебной коллегии по уголовным делам Оренбургского областного суда от 03.11.2016 по делу № 22-4229/2016 [Электронный ресурс]. URL: http://sudact.ru/regular/doc/pyDIbXPBiF1q/ (дата обращения: 20 сентября 2018 г.).

15. Апелляционное постановление Верховного суда Республики Саха (Якутия) от 27.08.2013 №22К-1644/2013 [Электронный ресурс]. URL: http://sudact.ru/regular/doc/2Zu9oah4YNQu/ (дата обращения: 20 сентября 2018 г.).

16. Яковлев А.Н. «Электронная» составляющая осмотра места происшествия // Библиотека криминалиста. Научный журнал. 2015. № 5. С. 281.

В.А. Мазуров,
кандидат юридических наук, доцент кафедры уголовного права и криминологии
Алтайский государственный университет, г. Барнаул

С.В. Новичихин,
магистрант
Алтайский государственный университет, г. Барнаул

К ВОПРОСУ О НЕКОТОРЫХ КРИМИНОЛОГИЧЕСКИХ ПРОБЛЕМАХ ПРОФИЛАКТИКИ КИБЕРПРЕСТУПНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

В настоящее время информационные технологии стали неотъемлемой частью жизни каждого цивилизованного человека. Их использование обусловлено различными причинами, начиная с удобства хранения и передачи информации на значительные расстояния с помощью глобальной сети «Интернет», заканчивая удовлетворением социальной потребности в общении. Активное развитие в XXI веке получил процесс глобализации, выражающийся в сближении государственных экономик, политических систем, правовых семей и т.д. Данный факт обусловил расширение отдельных видов преступлений, среди которых в первую очередь необходимо назвать терроризм, экстремизм, преступления в сфере компьютерной информации и другие. Главной особенностью данных правонарушений является их транснациональный характер, так, например, координация деятельности может осуществляться на территории одного государства, а возникающий в результате преступления ущерб локализуется на территории другой страны. Потерпевшими могут стать не только граждане, но и национальные компании, а иногда и государство в целом. В этой связи перед каждым государством встаёт задача по созданию системы правоохранительных мер, направленных на стабилизацию социального поля. Одной из «набирающих обороты» в последнее десятилетие стала киберпреступность. Нарастающая проблема слабой защищенности глобальных сетей от преступных деяний носит комплексный характер и имеет много составляющих (организационную, техническую, правовую, экономическую, социальную и др.), затрагивая не только международные, общие для всех стран, но и национальные интересы отдельных государств.

Согласно определению представленному В.А. Номоконовым под киберпреступностью следует понимать «совокупность преступлений, совершаемых в виртуальном пространстве с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, и против компьютерных систем, компьютерных сетей и компьютерных данных» [4, с. 45]. Развитию киберпреступности служит компьютеризация социальных отношений. Так, в России, например, в последние годы активное распространение получило развитие криптовалюты, так называемые «биткоины». Отсутствие чёткого нормативного регулирования данных общественных отношений вызвало благоприятную среду для развития преступности в данной сфере.

Непосредственному правовому регулированию киберпреступности посвящена глава 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации». По данным официальной статистики, представленным в отчёте Министерства внутренних дел Российской Федерации, за период с января по сентябрь 2018 года на территории Российской Федерации в указанный период совершено 1835 преступлений в сфере компьютерной информации, что на 26,3% больше, чем в 2017 году [7].

Рост преступлений данной направленности позволяет говорить о существовании в настоящее время криминологических проблем профилактики киберпреступности. На наш взгляд, данные проблемы обусловлены следующими факторами.

Одной из главных проблем криминологической профилактики киберпреступности является виктимное поведение граждан России, обусловлено правовой безграмотностью. Граждане, осваивая интернет сеть, зачастую, безразлично относятся к вводу личных данных и способах хранения информации, что создаёт благоприятную среду для совершения преступлений.

Решение данной проблемы необходимо проводить комплексно. Противодействие с киберпреступлениями входит в обязанности полиции, федеральных органов и отделов по борьбе с киберпреступностью и коммерческих организаций по обеспечению информационной безопасности. Мы считаем, что целесообразно начать с профилактики данных преступлений среди подростков, поскольку они наиболее активно подвержены влиянию со стороны взрослых и как следствие наиболее часто могут быть как потерпевшими, так и соучастниками в преступлениях.

В научной литературе мы можем встретить следующие рекомендации по профилактике киберпреступности у детей:

1. «Развивайте у подростков навыки критического мышления, объясните им, что в Интернете не вся информация правдива.
2. Используйте фильтры, блокирующие нежелательное содержание.
3. Не распространяй информацию о себе и своих родителях: видео, фото, адреса, телефоны, номер школы, состояние доходов семьи и т.п.
4. Не совершай противозаконных действий в интернете. Помни – это наказуемо Законом» [3].

Следующим шагом должно стать повышение киберграмотности среди учащихся высших учебных заведений, для этого предлагаем введение специальных дисциплин, например, таких как «Информационное право», «Основы кибербезопасности». Для студентов юридических факультетов и институтов дисциплину «Криминалистические особенности расследования киберпреступлений». Такая практика существует в институтах МВД и в единицах университетов нашей страны.

На сайте Следственного управления Следственного комитета Российской Федерации по Республике Адыгея представлены следующие Советы по предупреждению киберпреступлений:

1. Используйте лицензионное программное обеспечение для защиты от заражения компьютера или мобильного устройства при установке различных программ;
2. Установите антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и другую технику;
3. Не загружайте файлы из непроверенных источников;
4. Не переходите по ссылкам, содержащимся в спаме и других подозрительных электронных письмах отправителей, которых вы не знаете;
5. Воздержитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги [5].

Таким образом, необходимо отметить, что меры по профилактике осуществляются следственными органами и среди взрослого населения.

Также изучение судебной практики позволяет говорить о том, что в настоящее время отмечается высокая квалификация

киберпреступников. В отличие от обычного преступника, что действует в реальном мире, киберпреступник не использует традиционное оружие - нож или пистолет. Его арсенал - информационное оружие, все инструменты, которые используются для проникновения в сети, взлома и модификации программного обеспечения, несанкционированного получения информации или блокировки работы компьютерных систем. Это позволяет им не оставлять следов присутствия и своего пребывания на месте совершенного преступления. Очень часто потерпевший не подозревает о совершенном преступлении, а когда все-таки обнаруживает - проходит большое количество времени.

По нашему мнению, предложенные способы разрешения проблем профилактики киберпреступности в Российской Федерации в случае их успешной реализации окажут значительное влияние на повышение эффективности борьбы с киберпреступлениями. Однако, нельзя забывать, что преступления в сфере компьютерной информации в большинстве случаем носят международный характер. Данный факт обуславливает необходимость профилактики и развития законодательства на международном уровне.

Необходимо отметить, что в уголовное законодательство Российской Федерации в настоящее время внесены значительные изменения, улучшившие ситуацию в сфере противодействия компьютерным преступлениям. Несмотря на это, согласно мнению А.Г. Волеводз, нормативное регулирование киберпространства в одной отдельно взятой стране невозможно [1, с. 17]. Аналогичной позиции придерживается О.С. Гузеева: «наступление ответственности за совершение транснациональных преступлений, к которым относятся интернет - преступления, должно быть урегулировано международно-правовыми актами» [2, с. 77]. Для решения юридических, технических и организационных задач, связанных с обеспечением безопасности киберпространства требуется кооперация, координация и стратегическое партнерство всех заинтересованных в этом государств, среди которых активным участником является Россия.

На наш взгляд, упущением является тот факт, что в настоящее время Российская Федерация не подписала Европейскую Конвенцию по киберпреступности, оставив за собой право определиться с участием в Конвенции при установлении приемлемых для России условий трансграничного доступа к компьютерным сетям [6]. Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, которые бы учитывали

специфику информационных технологий, затрудняет формирование системы международной кибербезопасности. Сегодня как никогда необходима активизация международного взаимодействия по обеспечению кибербезопасности, а Российская Федерация может выступить инициатором разработки глобальной конвенции по борьбе с преступлениями в информационной сфере[8].

Таким образом, резюмируя вышеизложенное, можно сделать вывод о том, что разрешение проблем профилактики киберпреступности в Российской Федерации, напрямую зависит от международного сотрудничества в данной сфере, а также развития национального самосознания и развития. Информационные технологии стали важной составляющей жизни современного человека и отказ от них в целях предотвращения киберпреступлений является нецелесообразным, вектором развития Российской Федерации как демократического, правового государства является создания правового и информационного пространства способного адаптироваться к развитию общественных отношений.

Список литературы

1. Волеводз, А. Г. Конвенция о киберпреступности: новации правового регулирования // Правовые вопросы связи. – 2007. – № 2. – С. 17-25.

2. Гузеева, О.С. Уголовная политика в отношении преступлений, совершаемых в российском сегменте сети Интернет // Законы России: опыт, анализ, практика. – 2014. – № 6. – С. 74

3. Как обеспечить безопасность детей в сети интернет [Электронный ресурс] Режим доступа URL: http://okha7.ru/storage/app/uploads/public/568/e56/271/568e56271dff9777378179.pdf (дата обращения 04.12.2018)

4. Номоконов, В. А. Киберпреступность как новая криминальная угроза / В.А. Номоконов, Т.Л. Тропинина // Криминология: вчера, сегодня, завтра. — 2012. — № 1 (24). — С. 45-55.

5. Профилактика киберпреступлений [Электронный ресурс] Режим доступа: Официальный сайт Следственного управлении Следственного комитета Российской Федерации по Республике Адыгея URL: http://adygheya.sledcom.ru/about/divisions (дата обращения 01.12.2018)

6. Распоряжение Президента РФ от 22.03.2008 № 144-рп «О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. № 557-рп «О подписании Конвенции о

киберпреступности» // Собрание законодательства РФ. – 2008. – № 13. – Ст. 1295.

7. Состояние преступности в России за январь – сентябрь 2018 / [Электронный ресурс] Режим доступа: Официальный сайт Министерства внутренних дел Российской Федерации. URL: file:///C:/Users/Acer/Downloads/Sb_1809.pdf (дата обращения 04.12.2018)

8. Тарасенко В.В. Киберпреступность: международный уровень решения проблемы // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. XII междунар. студ. науч.-практ. конф. № 1(12). URL: https://sibac.info/archive/meghdis/1(12).pdf (дата обращения: 04.12.2018)

С.Р. Манукян,
заместитель начальника отдела экономической безопасности и противодействия коррупции УМВД России по ЗАТО Северск Томской области

ОПЫТ ЗАРУБЕЖНЫХ СТРАН ПО ПРОТИВОДЕЙСТВИЮ ЭКСТРЕМИСТСКИМ ДЕЯНИЯМ, СОВЕРШАЕМЫМ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Одним из средств совершенствования деятельности органов внутренних дел по профилактике и пресечению межнациональных и межрелигиозных конфликтов является заимствование опыта зарубежных стран. Его изучение помогает осуществить анализ состояния борьбы с правонарушениями определенного вида и скорректировать, при необходимости, программные документы по их профилактике и пресечению.

Стремительное увеличение в нашей стране числа экстремистских правонарушений, большая часть которых совершается с использованием информационно-телекоммуникационных сетей, включая «Интернет», обусловливает необходимость исследования возможности системного либо фрагментарного задействования достижений других государств, в том числе бывших союзных

республик, по противодействию экстремизму, совершаемому с применением современных информационных технологий.

С учетом стоящей перед российским обществом и государством задачи укрепления взаимодействия с населением в целях улучшения работы по профилактике преступлений следует рассмотреть опыт Великобритании. Отмечается, что созданное в ней специальное бюро по борьбе с экстремизмом и терроризмом в информационном пространстве призвало население сообщать об обнаруженных в сети «Интернет» материалов экстремисткой и террористической направленности путем нажатия имеющейся на веб-сайтах кнопки «Stop», после чего провайдеры должны сразу же адресовать пользователя на сайт, на котором его просят в анонимной форме обозначить веб-сайт, где был обнаружен такого рода материал. В течение полутора суток этот материал изучается, и при наличии в его содержании призывов к экстремизму и терроризму названное бюро обеспечивает, обращаясь к соответствующему провайдеру, удаление данного материала.

Кроме того, осуществление постоянной связи Национального британского бюро с европейским подразделением Интерпола – Европолом в данном направлении позволяет отслеживать с помощью общественности экстремистские публикации и публикации в поддержку терроризму, выполненные на четырех языках, и удалять их в те же самые сроки [1, с. 84].

Весьма полезным может быть опыт Соединенных Штатов Америки, хотя внедрение его в российское общество потребует весьма больших денежных средств, а также значительных политических и дипломатических усилий. Отмечается, что противодействие экстремизму в этой стране включает ряд направлений и организационных мероприятий. Так, прежде всего, коренным образом видоизменено миграционное законодательство. Кроме того, ведется постоянная работа по разъяснению опасности экстремизма и терроризма, для чего задействуются исследовательские научные и общественные центры, проводятся открытые для населения слушания в Конгрессе США, в которых участвуют не только правоохранительные органы, но и представители различных конфессий, прежде всего, ислама.

Нужность такого формата слушаний предопределяется тем, что идеологической платформой религиозного и тесно связанного с ним национального экстремизма, в том числе в России, является произвольное толкование доктрин ислама, а также исламского права. Имея немалые денежные средства, США реализуют такую программу

предупреждения экстремизма и терроризма, как участие в деятельности масс-медиа некоторых исламских государств, и такое участие достигает нередко двадцати пяти процентов вложений на функционирование медиа-групп [2, с. 100-101].

Востребованными для нашей страны являются подходы к взаимодействию органов внутренних дел и средств массовой информации. Так, в Германии существует правило, в соответствии с которым при совершении особо тяжких преступлений информация о проводимых полицией действий не подлежит опубликованию без согласования с руководством полиции.

Здесь же полезным является правило о едином федеральном удостоверении представителя прессы, что дает возможность установить автора публикации (сообщения). В целом можно говорить о надлежащей регламентации целого ряда правомочий средств массовой информации по информационному сопровождению деятельности полиции: фото– и видео-сообщения, создание передвижных пунктов для прессы и т.д. [3, с. 128-129].

Еще одно интересное установление существует в Великобритании, где общественная организация «Союз операторов Интернет» присваивает сайтам, в зависимости от соблюдения ими этических положений, определенные категории, указывающие, косвенно, на объективность подачи информации [4, с. 18].

Полезным для целей совершенствования деятельности органов внутренних дел России по профилактике межнационального и межрелигиозного экстремизма является опыт Республики Казахстан, в которой, в соответствии с законом от 10 июля 2009 года № 178-IV «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-телекоммуникационных сетей», все ресурсы, в том числе социальные сети, чаты, блоги, форумы и WAP-порталы приравниваются к традиционным средствам массовой информации. Такая правовая новелла означает, что в отношение отмеченных информационных ресурсов вводится запрет на размещение материалов экстремистского характера. Кроме того, может быть осуществлено судебное производство в отношение зарубежных средств массовой информации, имеющих свои представительства, при размещении в них таких материалов [5].

Однако главная причина слабой контролируемости сети Интернет с точки зрения профилактики и пресечения экстремизма состоит в том, что большинство сайтов, на которых постоянно размещаются экстремистские материалы, зарегистрированы за

пределами нашей страны, и в этом случае отсутствуют правовые основания для непосредственной идентификации источника распространения таких материалов, а также для прекращения деятельности самих сайтов.

В этой связи появляется необходимость создания соответствующего ресурсного обеспечения деятельности ОВД, одним из элементов которого является информационно-аналитическая система мониторинга информации, имеющейся в интернетовском пространстве, в соцсетях «Вконтакте», «Одноклассники», Twitter, Facebook, YouTube, Instagram, RuTube и др. Названная система работает с большим объемом (потоком) информации, используя для отбора необходимых сведений ключевые слова, указывающие на подготовку и совершение экстремистских актов. Отмечается необходимость улучшения технического обеспечения в виде специального программного обеспечения за счет приобретения зарубежных разработок, а также совершенствования, разработки нового отечественного программного продукта, применяемого территориальными Центрами по противодействию экстремизму, аналитическими подразделениями МВД России [6, с. 88].

Необходимость постоянного мониторинга имеющейся в интернет-пространстве информации с точки зрения относимости её к экстремистским материалам вызвана тем обстоятельством, что одним из критериев осложнения межнациональных и межрелигиозных отношений в определенных частях страны является значительное возрастание публикаций в интернетовской среде, которое, наряду с увеличением числа слухов в виде листовок, публикаций в средствах массовой информации, а также выступлений на митингах с призывами к радикальным действиям, требует немедленного реагирования со стороны общества и государства, в том числе органов внутренних дел.

Список литературы

1. Долгошеин П.С. Специфика противодействия проявлениям экстремизма и терроризма в сети Интернет в Европейском союзе и Российской Федерации // Противодействие экстремизму и терроризму: мат-лы Межд. науч.-практ. конф. (Москва, 7 июня 2017 года) / под.общ. ред. А.М. Багмета. М.: Московская академия Следственного комитета Российской Федерации. 2017. С. 82-85.

2. Карпович О.Г. Опыт противодействия терроризму в США // Противодействие экстремизму и терроризму: мат-лы Межд. науч.-практ. конф. (Москва, 7 июня 2017 года) / под.общ. ред. А.М. Багмета.

М.: Московская академия Следственного комитета Российской Федерации. 2017. С. 99-105.

3. Сойников С.А. Административно-правовое регулирование оборота массовой информации в органах внутренних дел Федеративной Республики Германия // Научный портал МВД России. 2011. № 2 (14). С. 124-128.

4. Коневская О.Ю. Этические нормы и общественный контроль в правовом механизме предупреждения злоупотреблений свободой массовой информации // Труды Академии МВД России. 2012. № 4 (24). С. 16-20.

5. Закон Республики Казахстан от 10 июля 2009 года № 178-IV «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информационно-телекоммуникационных сетей» // http://adilet.zan.kz/rus/docs/Z090000178_

6. Баранов В.В. К вопросу о построении автоматизированной информационно-аналитической системы поддержки принятия решений руководителя органа внутренних дел в сфере борьбы с экстремизмом // Труды Академии управления МВД Росси. 2014. № 3 (31). С. 87-90.

Н.А. Морозова,
доцент кафедры уголовного права и уголовного процесса третьего факультета повышения квалификации
Московская академия Следственного комитета Российской Федерации, г. Новосибирск

М.В. Галдин,
доцент кафедры уголовного права и уголовного процесса третьего факультета повышения квалификации
Московская академия Следственного комитета Российской Федерации, г. Новосибирск

НЕКОТОРЫЕ СЛОЖНОСТИ В КВАЛИФИКАЦИИ И ОРГАНИЗАЦИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ПОЛОВОЙ НЕПРИКОСНОВЕННОСТИ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ, И ПУТИ ИХ ПРЕОДОЛЕНИЯ

В современном обществе межличностное общение все больше приобретает виртуальный характер, поглощается информационными технологиями. Социальные сети стали сегодня самым быстрым, простым и удобным способом общения. К сожалению, любым достижениям науки и техники неизменно сопутствуют правонарушения.

Общение взрослых с детьми в социальных сетях под вымышленными именами на сексуальные темы, обмен фотоизображениями и видеороликами порнографического содержания, просьбы выслать собственные фотографии в обнаженном виде – вот далеко не полный перечень способов развращения несовершеннолетних с использованием телекоммуникационной сети Интернет. Кроме такого общения практикуются более личные контакты посредством различных мессенджеров (например, «WhatsUp», «Viber», «Skype»).

В соответствии со ст. 22 Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений от 25.10.2007 [1], ратифицированной федеральным законом от 07 мая 2013 года [2] каждая из Сторон принимает необходимые законодательные и иные меры для введения уголовной ответственности лиц за умышленное склонение ребенка в сексуальных

целях к наблюдению сексуального насилия или деятельности сексуального характера, даже если они физически в них не участвуют.

Российским уголовным законом установлен шестнадцатилетний возраст привлечения таких лиц к уголовной ответственности. Перечисленные деяния подлежат квалификации по ст. 135 УК РФ как развратные действия. В качестве примера может быть приведено уголовное дело в отношении М., который посылал тринадцатилетней девочке фотографии с изображениями сексуального характера, а также обменивался текстовыми сообщениями такого же характера в социальной сети. В отношении М. судом вынесен приговор по ч. 2 ст. 135 УК РФ [3]. Если развратные действия совершены в отношении не достигшего двенадцатилетнего возраста ребенка, то деяние признается иными насильственными действиями сексуального характера и квалифицируется по п. «б» ч. 4 ст. 132 УК РФ.

Причина переквалификации развратных действий в иные насильственные действия сексуального характера обосновывается в примечании к ст. 131 УК РФ. Признавая соответствие уголовного закона Основному закону нашего государства, Конституционный Суд Российской Федерации указал, что потерпевшее лицо в силу психологической незрелости не осознает в полной мере характер совершаемых с ним действий и их физические, нравственные, психологические, социальные и иные последствия (лишение подростка детства и отрочества, торможение личностного развития, сокращение его социальных перспектив, препятствие получению образования) и, соответственно, выступает жертвой осознанных и волевых действий совершеннолетнего лица [4]. Так, по приговору Московского городского суда признан виновным М. по п. «б» ч. 4 ст. 132 УК РФ, который в социальной сети общался с десятилетней жительницей другого региона и отправлял текстовые, графические, фото и видео-файлы порнографического содержания для побуждения к сексуальным отношениям [5].

На рассмотрении суда в республике Татарстан в настоящее время находится уголовное дело в отношении тридцатитрехлетнего жителя Альметьевска, обвиняемого в совращении пятидесяти шести детей. По версии следствия, он создал в социальных сетях две страницы на имя одиннадцатилетнего мальчика и четырнадцатилетней девочки и стал знакомиться с детьми, уговаривая тех снимать себя на фото- и видеокамеру в непристойном виде. Получив записи и угрожая их распространением, подсудимый требовал присылать ему новые или настаивал на встрече [6].

Развитие интернет-технологий предоставляет огромные возможности по общению. Их использование в качестве средства совершения преступлений делает пространственные границы прозрачными. Выявление, раскрытие, расследование и последующее рассмотрение в суде уголовных дел о таких преступлениях сопряжено с возникновением многочисленных проблем. В досудебном производстве по уголовным делам нередко возникают споры о месте производства по уголовному делу. Особую важность тому придает часть первая ст. 47 Конституции РФ, в соответствии с которой «никто не может быть лишен права на рассмотрение его дела в том суде и тем судьей, к подсудности которых оно отнесено законом».

В соответствии со ст. 152 УПК РФ предварительное расследование производится по месту совершения деяния, содержащего признаки преступления, за исключением следующих случаев. При необходимости производства следственных или розыскных действий в другом месте следователь вправе произвести их лично либо поручить производство этих действий следователю или органу дознания, дознаватель вправе произвести их лично, либо поручить производство этих действий дознавателю или органу дознания. Если преступление было начато в одном месте, а окончено в другом месте, то уголовное дело расследуется по месту окончания преступления. Если преступления совершены в разных местах, то по решению вышестоящего руководителя следственного органа уголовное дело расследуется по месту совершения большинства преступлений или наиболее тяжкого из них. Предварительное расследование может производиться по месту нахождения обвиняемого или большинства свидетелей в целях обеспечения его полноты, объективности и соблюдения процессуальных сроков. Согласно последним дополнениям этой статьи, если преступление совершено вне пределов РФ, то уголовное дело расследуется по основаниям, предусмотренным статьей 12 УК РФ, или в соответствии со статьей 459 УПК РФ по месту жительства или месту пребывания потерпевшего в РФ, либо по месту нахождения большинства свидетелей, либо по месту жительства или месту пребывания обвиняемого в РФ, если потерпевший проживает или пребывает вне пределов РФ.

Однако наличие подробного описания правил определения места производства расследования не решает всех возникающих на практике проблем. Подтверждением тому служит частое возникновение и неоднозначное разрешение вопросов о территориальной подследственности уголовных дел о совершении

лицами преступлений против половой неприкосновенности несовершеннолетних, находящихся на территории различных субъектов РФ с использованием сети Интернет. Такие преступления могут быть совершены лицами за пределами РФ. Организация дальнейшего расследования может иметь различные направления.

Согласно первому из возможных вариантов, в следственное подразделение субъекта РФ по месту регистрации IP-адреса (ID-адреса) направляется поручение в целях установления несовершеннолетнего и его допроса в качестве свидетеля. После получения материалов исполненного поручения, следователь возбуждает уголовное дело и направляет повторное поручение о допросах несовершеннолетнего потерпевшего, его законных представителей в качестве свидетелей, а также о производстве комплексной психолого-психиатрической судебной экспертизы и иных процессуальных действиях.

Недостатками такого подхода является то, что расследование одного эпизода затягивается на 3-4 месяца, что может быть сочтено неэффективной организацией расследования и, как следствие, нарушением разумного срока судопроизводства. При таком подходе, на наш взгляд, страдают правила определения места производства предварительного расследования. Ведь уголовное дело возбуждается не по месту совершения преступления и не по месту жительства либо пребывания обвиняемого или потерпевшего, как того требует закон, а по месту размещения органа расследования. Кроме этого, не вполне верным представляется допрос несовершеннолетнего, которому причинен вред в результате совершения преступления, в качестве свидетеля. Повторность допроса несовершеннолетнего противоречит нормам международного права и ведомственным нормативно-правовым актам Следственного комитета РФ о недопустимости необоснованного неоднократного производства следственных действий с участием несовершеннолетнего, необходимости тщательной подготовки к следственным действиям и получении от несовершеннолетнего информации в максимально щадящем режиме без ущерба для доказывания [7].

Следование другой стратегии расследования позволяет сократить срок расследования более чем в два раза. В соответствии с ним, после получении сведений о совершении находящимся за пределами РФ подозреваемым или обвиняемым преступления в другом субъекте РФ, следователь выделяет материалы об этом в отдельное производство. Получивший их следователь производит уголовно-процессуальную проверку в предусмотренном ст. ст. 144-145

УПК РФ порядке и при наличии оснований возбуждает уголовное дело. После проведения необходимых процессуальных действий по нему направляет его для присоединения к основному уголовному делу. Такая практика в целом соответствует сложившейся практике выделения уголовного дела в отдельное производство для завершения предварительного расследования в случаях, когда это вызвано большим объемом уголовного дела или множественностью его эпизодов (ст. 154 ч. 2 УПК РФ).

При всей целесообразности применения второго из названных вариантов организации расследования, для закрепления его на практике, на наш взгляд, необходимо внесение изменений в часть первую ст. 155 УПК РФ, которая содержит обязательное условие: выделение допускается лишь тогда, когда становится известно о совершении иными лицами преступления, не связанного с расследуемым преступлением. При этом, Конституционный Суд РФ неоднократно обращал внимание на то, что указанная норма уголовно-процессуального закона не содержит правовой неопределенности [8]. Более того, в одном из своих решений Конституционный Суд РФ указал, что ст. 155 УПК РФ не содержит положений, позволяющих выделять материалы в отношении подозреваемых или обвиняемых в совершении преступления по расследуемому уголовному делу [9].

С учетом такого толкования практика применения ст. 155 УПК РФ требует внесения соответствующих изменений, без которых следование второму из изложенных вариантов организации расследования может быть признано не соответствующим букве закона. Кроме того, не исключено возникновение вполне резонного вопроса: зачем материалы о совершенном преступлении выделять, если в последующем потребуется соединять их в одно производство с основным расследуемым уголовным делом?

Анализ выявленных недостатков первых двух вариантов стимулирует на поиск другого варианта организации расследования дополнительного эпизода преступной деятельности лица в отношении несовершеннолетнего, который бы в большей степени согласовывался с действующим законодательством. В этом отношении наиболее оптимальнымнам представляется следующий порядок действий. При поступлении сведений о том, что подозреваемый или обвиняемый с использованием сети Интернет общался с несовершеннолетним, проживающим в другом субъекте РФ, следователь в соответствии со ст.143 УПК РФ составляет рапорт об обнаружении признаков преступления, к которому в копиях прилагает материалы уголовного дела и направляет его по подследственности. В случае обнаружения по

месту жительства несовершеннолетнего достаточных данных о признаках преступления, следователь возбуждает уголовное дело и производит допросы несовершеннолетнего потерпевшего, его законного представителя, свидетелей, назначает судебные экспертизы и выполняет иные необходимые процессуальные действия. По их завершении уголовное дело о дополнительном эпизоде преступной деятельности может быть направлено для соединения с основным уголовным делом.

К достоинствам предлагаемого нами варианта отказа от использования института выделения в отдельное производство материалов уголовного дела следует отнести его простоту, минимизацию затрат по передаче информации о совершенном преступлении по месту нахождения потерпевшего, а также предоставление всей полноты процессуальной самостоятельности следователю. В качестве его единственного недостатка следует указать лишь то, что третий пункт ч. 1 ст.145 УПК РФ допускает передачу сообщения по подследственности в соответствии со ст. 151 УПК РФ, то есть по подведомственности. На данное обстоятельство уже обращалось внимание на необходимость дополнения этой нормы ст. 145 УПК РФ ссылкой на ст.152 УПК РФ, что будет отражать многолетнюю правоприменительную практику [10, с. 50].

Полагаем, что разрешение освещенных в настоящей статье небесспорных вопросов представляет интерес для следственных работников и ученых, а также содержит сведения для дальнейшего совершенствования действующего законодательства.

Список литературы

1. Конвенция Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений» (CETS 201) [рус., англ.] (Заключена в г. Лансароте 25.10.2007) // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / Компания «Консультант Плюс». – М., 2018.

2. Федеральный закон от 07.05.2013 N 76-ФЗ «О ратификации Конвенции Совета Европы о защите детей от сексуальной эксплуатации и сексуальных злоупотреблений» // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / Компания «Консультант Плюс». – М., 2018.

3. URL: https://http://sudact.ru/region-sverdlovskaya-oblast-s/vidprugolovnoe/jurisdiction-fed/section-acts/

4. URL:http://legalacts.ru/doc/opredelenie-konstitutsionnogo-suda-rf-ot-21102008-n-568-o-o-ob/

5. Житель Красноярска приговорен к 16 годам тюрьмы за серию развратных действий в отношении детей // Пресс-служба ГУ МВД России по Красноярскому краю // Официальный сайт главного управления МВД России по Красноярскому краю. URL: http://24.mvd.ru/news/item/1194539

6. URL:https://ria.ru/incidents/20171129/1509785749.html

7. Указание Первого заместителя Генерального Прокурора РФ – Председателя Следственного комитета при прокуратуре РФ от 16 марта 2010 № 2/206 О введении специализации следователей Следственного комитета при прокуратуре Российской Федерации по расследованию преступлений, совершенных в отношении несовершеннолетних» // URL:https://sledcom.ru/documents/base

8. Определение Конституционного Суда РФ от 05.06.2014 N 1534-О«Об отказе в принятии к рассмотрению жалобы гражданина Щапова Юрия Степановича на нарушение его конституционных прав положениями статей 30, 34, 36, 38, 42, 125, 140, 141, 144, 145, 155, 237 и 239 Уголовно-процессуального кодекса Российской Федерации» // Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / Компания «Консультант Плюс». – М., 2018.

9. Определение Конституционного Суда РФ от 27.06.2017 N 1252-О «Об отказе в принятии к рассмотрению жалобы гражданина Остапенко Максима Юрьевича на нарушение его конституционных прав положениями статей 38, 155 и 217 Уголовно-процессуального кодекса Российской Федерации»Консультант Плюс. Законодательство. ВерсияПроф [Электронный ресурс] / Компания «Консультант Плюс». – М., 2018.

10. Ряполова, Я.П. Процессуальные действия прокурора по надзору за законностью и обоснованностью действий и решений на стадии возбуждения уголовного дела / Я. П. Ряполова // Российский следователь. – 2012. – N 14. – С. 9 - 11.

В.В. Поляков,
кандидат юридических наук; доцент кафедры уголовного процесса и криминалистики
Алтайский государственный университет, г. Барнаул

А.В. Ширяев,
аспирант кафедры уголовного процесса и криминалистики
Алтайский государственный университет, г. Барнаул

КРИМИНАЛИСТИЧЕСКИЕ АСПЕКТЫ ЛИЧНОСТИ ПОТЕРПЕВШИХ ОТ КИБЕРПРЕСТУПЛЕНИЙ

Современные компьютерные технологии, использующие возможности телекоммуникационных сетей связи, позволяют совершать операции, которые ранее были немыслимы, как, например, электронные платежи и операции с ценными бумагами, удаленное управление техническими устройствами. Эти технологии быстро внедряются в практику, при этом вопросы, связанные с безопасностью их использования, решаются с запозданием. В результате распространение получают неправомерные действия со стороны компьютерных преступников. Нужно полагать, что с дальнейшим ростом компьютеризации число потерпевших будет увеличиваться до тех пор, пока не будут разработаны и применены эффективные меры противодействия этому явлению [1].

Одним из важных криминалистических аспектов в расследовании и предотвращении компьютерных преступлений является комплексное исследование специфических особенностей личности потерпевших, поскольку именно эти особенности в значительной мере способствуют преступным посягательствам. Несмотря на свою актуальность, тема формирования и анализа современной криминалистической характеристики личности потерпевших от киберпреступлений исследована явно недостаточно. Большей частью в научных работах освещен криминологический портрет, криминалистическая и уголовно-правовая характеристики киберпреступников [2]. Следует отметить, что за рубежом степень проработанности вопросов характеристики личности потерпевших от киберпреступлений выше, чем в России [3, 4]. В настоящей работе на основе анализа судебно-следственной практики Российской Федерации, анкетирования сотрудников правоохранительных органов и специалистов в сфере компьютерной информации проводится

исследование криминалистических аспектов именно личности потерпевших.

Отметим, что проведение исследований в области личности компьютерных преступников представляет определенные сложности в силу латентности киберпреступности и специфического поведения самих потерпевших, которые зачастую не желают проведения расследования [5]. Для изучения реальной ситуации по потерпевшим от компьютерных преступлений значение имеет не только сбор и анализ судебно-следственной практики, но и информации по невыявленным преступлениям, например, с помощью анкетирования различных категорий респондентов, связанных с информационной безопасностью и расследованием данных преступлений. Большое значение имеет разработка и использование современных информационных технологий, позволяющих на автоматизированном уровне собирать данные, входящие в криминалистическую характеристику компьютерных преступлений, в частности, на основе технологии honeypot [6].

Актуальность комплексного исследования компьютерной преступности может быть проиллюстрирована тем, что, по данным ежегодного исследования Norton Cybercrime Report, в России около 56% пользователей старше 18-лет стали жертвами компьютерных преступлений, 71% пользователей мобильных устройств получили вредоносное программное обеспечение с текстовыми сообщениями от неизвестных лиц с предложением перейти по неизвестной ссылке или набрать незнакомый номер, у 47% пользователей были взломаны аккаунты с личной информацией, 19% пользователей стали жертвами спама или фальшивых ссылок в социальных сетях [7]. Факторы распространения киберпреступности, и, как следствие, увеличения числа потерпевших, можно систематизировать. Основными из них являются следующие:

- отставание правового регулирования общественных отношений, связанных с компьютерными преступлениями;
- недостаточная работа по криминалистическому предупреждению совершения киберпреступлений;
- разрыв между техническим уровнем знаний, подготовки, образования киберпреступников и уровнем подготовки, образования, бдительности потерпевших от данного вида преступлений;
- объединение пользователей в преступные группы, имеющие хорошо организованную основу, с целью получения материальной выгоды или преследования иных общих интересов, например, экстремистского характера. При этом такие группы и сообщества

могут иметь значительную численность, а их деятельность может носить транснациональный характер;

- общий рост количества пользователей, в том числе пренебрегающих защитой компьютерной информации;

- рост числа недостаточно защищенных объектов информатизации, содержащих компьютерную информацию, представляющую ценность для преступников;

- недостаточный уровень квалификации сотрудников правоохранительных органов, участвующих в расследовании и предупреждении компьютерных преступлений, а также отставание их квалификации от лиц, совершающих данные преступления, особенно высокотехнологичными способами;

- недостаточная материально-техническая база правоохранительных органов, необходимая для противодействия современной киберпреступности;

- недостаточная координация и сотрудничество между правоохранительными органами как внутри государства, так и за его пределами [8].

Обобщение имеющейся судебно-следственной практики и результатов проведенного нами анкетирования сотрудников правоохранительных органов, а также анализ научной литературы позволило выявить общие черты и сформировать классификацию потерпевших от киберпреступлений. Криминалистическое классифицирование может быть проведено на основе выделения различных критериев [9].

1. По характеру причиненного вреда (различные виды материального (имущественного) вреда, моральный вред, физический вред).
2. По наличию специальных знаний и навыков в сфере информационных технологий.
3. По биофизиологическим характеристикам.
4. По характеру взаимоотношений с преступником (отношения случайные, заранее определенные, виктимные).
5. По содействию расследованию преступлений.

1. Классификация по характеру причиненного вреда. Принципиальным представляется, что выделяемые группы потерпевших различаются в зависимости от характера причиненного вреда. Наиболее распространены компьютерные преступления, наносящие потерпевшим имущественный ущерб. Компьютерная информация может представлять существенную ценность, в силу этого при неправомерном доступе к ней, приводящем к ее модификации,

копированию, блокированию или уничтожению, может наноситься непосредственный материальный ущерб собственнику этой информации. В качестве примера можно привести хищение денежных средств с банковских карт потерпевших путем модификации преступниками компьютерной информации в платежных системах.

Моральный вред причиняется потерпевших, как правило, в результате неправомерного доступа к компьютерной информации, которая носит личный характер. В настоящее время распространенными формами нанесения морального вреда является незаконный доступ к аккаунтам социальных сетей или к электронной почте пользователей. Повсеместное распространение социальных сервисов сети Интернет порождает новые формы антиобщественного поведения. Одним из примеров такого поведения является так называемый «троллинг» [10], который, на наш взгляд, не может быть отнесен к компьютерным преступлениям, если он не связан с неправомерным доступом к компьютерной информации или в нем не задействовано вредоносное программное обеспечение.

В результате действий компьютерных преступников может быть причинен не только моральный, но и физический вред здоровью граждан. Это может произойти при выведении из строя компьютерной техники учреждений здравоохранения, транспорта и т.д.

2. Классификация по наличию специальных знаний и навыков в сфере информационных технологий. По уровню использования компьютерных технологий потерпевших можно подразделить на следующие основные группы:

- недостаточно разбирающиеся в компьютерных технологиях. К их числу обычно относятся люди старших возрастных групп, а также лица с низким уровнем образования;

- относительно компетентные, но халатно относящиеся к обеспечению информационной безопасности объекта информатизации, содержащего конфиденциальную или охраняемую законом информацию. Такие граждане имеют достаточные знания, умения и навыки, а также материально-технические возможности по обеспечению защиты информации, однако пренебрегают этой защитой в силу непонимания реального уровня угроз;

- хорошо разбирающиеся в вопросах зашиты информации и принимающие меры к ее обеспечению. Сюда относится достаточно широкий круг лиц, начиная от специалистов, работающих в сфере информационных технологий, и заканчивая рядовыми пользователями.

Наиболее распространенной является первая группа потерпевших, в отношении которых преступления происходят из-за

недостаточных знаний способов и средств защиты компьютерной информации. Так, в 2014 г. в г. Барнауле преступник с помощью принадлежащего ему компьютера получил учетную запись и пароль к электронному почтовому ящику, принадлежащему потерпевшей. В качестве способа совершения преступления использовался прием, когда пароль был получен с помощью угадывания секретного вопроса**,** ответ на который был легко подобран с помощью данных о жизни потерпевшей, которые было не сложно получить. В дальнейшем это позволило преступнику осуществить неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в электронном почтовом ящике, и модифицировать ее.

3. Классификация по биофизиологическим характеристикам. Возрастные характеристики потерпевших существенно зависят от вида и характера компьютерного преступления. Наиболее активное использование компьютерных технологий приходится на возрастную группу до 35-40 лет, а средний возраст потерпевших составляет около 30 лет [11]. Материальный вред чаще наносится представителям старших возрастных групп, отличающихся более низкой компьютерной грамотностью. Именно они наиболее уязвимы в отношении различных видов мошенничества, совершаемых путем удаленного доступа с помощью информационных сетей, а также становятся жертвами вредоносных компьютерных атак.

Нужно также отметить, что, как и в случае компьютерных преступников, конкретные количественные данные в случае потерпевших могут различаться по регионам проживания, этот вопрос требует специального дополнительного исследования [12].

4. Классификация по характеру взаимоотношений с преступником. Потерпевшие от компьютерных преступлений могут быть выбраны преступниками целенаправленно или стать жертвами случайно. Для первой из этих групп потерпевших более свойственно личное знакомство с преступником, который выбирает их на основе знания каких-то личных данных. Жертвы могут представлять интерес для преступников по различным причинам: межличностным, например, ревность, личная неприязнь [13]; политическим, например, когда потерпевшим становится крупный общественный или государственный деятель [14, 15, 16]; экономическим, например, при конкуренции желании навредить деловой репутации; а также по многим другим причинам и поводам [17].

Анализ судебно-следственной практики показал, что в случае преступлений корыстной направленности основную группу составляют случайные потерпевшие. В качестве примера можно

привести дела о так называемом «фишинге», когда преступники получают конфиденциальные данные о потерпевших путем проведения массовых рассылок электронных писем или сообщений внутри различных онлайн-сервисов от имени благонадежных источников, например, банков. Несмотря на распространенность данной группы, важно отметить, что около 95% таких преступлений остаются в зоне латентности [18]. Достаточно часто случайными потерпевшими становятся владельцы сайтов, на которых происходит блокирование или замена содержимого, при этом выбор сайта для преступников является не принципиальным [19].

Встречаются случаи, когда случайными потерпевшими выступает неопределенный круг лиц, например, когда в их интересах действует прокурор, обращающийся с заявлением о признании информации, размещенной на сайте или интернет-странице, запрещенной к распространению на территории Российской Федерации [20].

Представляется важным выделение отдельной группы потерпевших, у которых преобладают виктимные свойства личности. В отличие от случайных потерпевших такие жертвы активно провоцируют совершение компьютерного преступления в отношении себя. В качестве примера, к их числу могут относиться лица, публично высказывающиеся негативно о «хакерах».

5. Классификация по содействию расследованию преступления. Данный вид классификации обусловлен спецификой компьютерных преступлений, заключающейся в следующем. Среди потерпевших может быть выделена достаточно многочисленная группа, для которой характерно такое парадоксальное поведение, как сокрытие обстоятельств преступления и даже противодействие его расследованию. Такие потерпевшие стремятся как можно скорее примириться с преступниками на стадии предварительного или судебного следствия для скорейшего прекращения уголовного дела. В качестве примера приведем случай из судебной практики, когда преступник, находясь у себя дома, осуществлял неправомерный удаленный доступ к компьютерной информации, собирал сведения, составляющие коммерческую тайну, и причинял имущественный ущерб без признаков хищения. На подготовительной части судебного заседания со стороны представителей потерпевших были заявлены ходатайства о прекращении уголовного дела в связи с примирением. Они ссылались на такой повод, как отсутствие моральных и материальных претензий, считая вред заглаженным полностью [21]. Отметим, что примирение в таких случаях может быть притворным, а

вред заглаживаться либо символически, либо в несоответствующем действительности объеме. Противодействие расследованию со стороны потерпевших может выражаться в уничтожении следов преступления, сокрытии реального ущерба, предоставлении правоохранительным органам только части криминалистически значимой информации и в иных формах [22]. Объяснение такого поведения потерпевших заключается в том, что разглашение сведений о низкой защищенности конфиденциальной информации, доверенной им, может привести к причинению вреда их деловой репутации, к утечке конфиденциальной информации в процессе следствия и судопроизводства, в страхе перед расследованием, которое в случае должностных лиц способно выявить их профессиональную непригодность. Другой распространенной причиной противодействия расследованию со стороны потерпевших является то, что в их компьютерной технике часто незаконно установлено нелицензионное программное обеспечение.

В заключение отметим, что исследование личности потерпевших необходимо осуществлять регулярно, так как многие криминалистически значимые черты потерпевших меняются вместе с динамично изменяющейся киберпреступностью. Полученные и систематизированные данные о потерпевших по компьютерным преступлениям имеют важное тактическое значение, способствуют повышению результативности оперативной и следственной работы, а также позволяют разработать необходимые меры криминалистического предупреждения данных преступлений.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №16-33-01160-ОГН.

Список литературы

1. Мазуров, В.А. Криминолого-криминалистическое предупреждение преступности в сфере высоких информационных и телекоммуникационных технологий / В.А. Мазуров, В.В. Поляков // Известия Алтайского государственного университета. – 2009. – № 2. – С. 95 - 98.

2. Поляков, В.В. Характеристика личности киберпреступников / В.В. Поляков, Н.В. Людкова // Теоретические и практические проблемы организации раскрытия и расследования преступлений: сб. мат. Всерос. науч. практ. конф. 22 апреля 2016 г.; - Хабаровск: ДВЮИ МВД России. - С. 250-255.

3. Герке, М. Понимание киберпреступности – явление, задачи и законодательный ответ [Электронный ресурс] // Международный союз электросвязи. 2014. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime2014_R.pdf (дата обращения 30.09.2018).

4. Ларина, Е.С. Кибервойны XXI века: о чем умолчал Эдвард Сноуден / Е.С. Ларина, В.С. Овчинский; Изборский клуб. – М.: Кн. мир, 2014. - 349 с.

5. Поляков, В.В. Анализ обстоятельств, затрудняющих расследование и доказывание преступлений в сфере компьютерной информации / В.В. Поляков // Уголовно-процессуальные и криминалистические чтения на Алтае : матер. Региональной науч.-практ. конф. / под ред. В.К. Гавло. – Барнаул : Изд-во Алт. ун-та, 2006. – Вып. 6. – С. 111-117.

6. Поляков, В.В. Система honeypot как инструмент сбора информации для противодействия киберпреступности / В.В. Поляков // Библиотека криминалиста : научный журнал. – 2017. – №1 (30). – С. 250-254.

7. Итоги исследования: Киберпреступность в России и мире // Rb.ru: информационный сайт 18.09.2012. URL:https://rb.ru/news/itogi-issledovaniya-kiberprestupnost-v-rossii-i-mi/ (дата обращения 30.09.2018).

8. Рассолов, И.М. Право и Интернет: теоретические проблемы / И.М. Рассолов. - М.: Норма, 2003. - 331 с.

9. Ахмедшин, Р.Л. Криминалистическая характеристика личности преступника. - Томск: Изд-во Том. ун-та, 2005. - 210 с.

10. Дементьев, О.М. Интернет - троллинг - шалость, правонарушение или преступление? / О.М. Дементьев, М.М. Дубровина // Science Time. - 2015. - № 10 (22). - С. 80-86.

11. Федоренко В.И. Виктимологический аспект преступлений в сети Интернет. URL: https://zakon.ru/blog/2012/1/19/viktimologicheskij_aspekt_prestuplenij_v_seti_internet (дата обращения 20.10.18).

12. Поляков, В.В. Региональные особенности криминалистической характеристики преступлений в сфере компьютерной информации / В.В. Поляков // Региональные аспекты технической и правовой защиты информации : монография / В.В. Поляков, В.А. Трушев, И.А. Рева, Вит.В. Поляков, П.В. Малинин и др. – Барнаул : Изд-во Алт. ун-та, 2013. – Гл. 1. – С. 9-42.

13. Уголовное дело № 1-308/2016 по ст. ч.1 ст.138, ч.1 ст.272 УК РФ) // Архив Московского районного суда г. Твери, 2016 г.

14. Россия и вызовы цифровой среды: рабочая тетр. / [В.С. Овчинский и др.]; [гл.ред. И.С. Иванов]; Российский совет по международным делам (РСМД). – М.: Спец-книга, 2014. – 40 с.

15. Стельмах, А.П. Кибернетическая безопасность: понятие и сущность феномена / А.П. Стельмах, А.В. Тонконогов // Социально-гуманитарные знания: научно-образовательное издание, 2013. - № 2. - С. 103-115.

16. Федотов, Н.Н. Форензика – компьютерная криминалистика. - М.: Юридический Мир, 2007.-360 с.

17. Уголовное дело № 1- 178/2016 (по ст. ч.1 ст. 272, ч.1 ст. 273 УК РФ) // Архив Харабалинского районного суда Астраханской области, 2016 г.

18. Старичков, М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристика: автореф. дис. … канд. юрид. наук / М.В. Старичков. - Иркутск, 2006. – С. 3.

19. Дефейс // Википедия. URL: http://ru.wikipedia.org/?oldid=86406971 (дата обращения: 07.07.2017).

20. Уголовное дело № 2-99/2017 (по ч. 1 ст. 272 УК РФ) // Архив Сковородинского районного суда Амурской области, 2017 г.

21. Уголовное дело №1-472/06 // Архив Железнодорожного районного суда г. Барнаула, 2006 г.

22. Погодин, С.Б. Особенности расследования преступлений в сфере компьютерной информации / С.Б. Погодин // Российский следователь. - 2004. - № 7. - С. 6 –9.

И.М. Проскурин,
адъюнкт
Барнаульский юридический институт МВД России, г. Барнаул

НЕКОТОРЫЕ ХАРАКТЕРНЫЕ ЧЕРТЫ ЛИЧНОСТИ ПРЕСТУПНИКОВ, СОВЕРШАЮЩИХ МОШЕННИЧЕСТВА В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Эффективная борьба с преступностью обеспечивается использованием оперативными аппаратами научных положений, разработанных теорией ОРД и апробированных правоприменительной практикой, связанных с познаниями закономерностей подготовки,

совершения и сокрытия преступлений, выявления признаков этих преступлений и особенностей их раскрытия [1, с. 115]. Исходной методологической основой для этих целей служит совокупность данных, характеризующих совершенные преступления. Эту совокупность принято называть оперативно-розыскной характеристикой преступлений [2].

Иными словами, не поняв и не уяснив суть механизма совершения того или иного преступления, крайне сложно своевременно и эффективно противодействовать его совершению, а если оно совершено, то принимать меры по его выявлению, раскрытию и содействию органам предварительного расследования по сбору доказательственной базы по уголовному делу.

Исходя из того, что любая характеристика это «описание отличительных качеств, свойств, черт, кого/чего-нибудь» [3] в теории ОРД введено и получило распространение понятие «оперативно-розыскная характеристика преступлений» для обозначения обобщенных сведений о преступлениях определенного вида. Оперативно-розыскная характеристика является неотъемлемым элементом частных методик раскрытия преступлений.

Следует отметить, что по вопросу понятия, определения, сущности и содержания оперативно-розыскной характеристики преступлений (ОРХП) нет единства взглядов [2]. Так, например, Белкин Р.С. считает, что «содержание этой «характеристики» еще более эклектично, нежели характеристики криминалистической. Здесь данные и уголовного права, и криминологии, включая даже уголовную статистику о динамике преступлений конкретного вида, что уж никак не должно иметь места в научной абстракции (а всякая характеристика преступления — это научная абстракция, поскольку отражает только типичное и устойчивое в преступлении), и практически в полном объеме то, что составляет стержень криминалистической характеристики — данные о типичных способах преступления и их следах Ничего оперативно-розыскного такая характеристика не содержит, она не имеет не только практического, но и научного смысла» [4, с. 223-224].

Существуют и другие мнения. Так, Б.В. Борин под оперативно-розыскной характеристикой понимает совокупность сведений о преступлениях определенного вида, на основании которых можно достаточно четко и ясно представить механизм их совершения, лиц, их совершивших, документы, используемые для совершения и т.п., что, в свою очередь, позволяет наметить и осуществить различные оперативно-розыскные мероприятия и меры по выявлению,

документированию указанных преступлений, то есть получению потенциальных доказательств совершения преступления [2].

Данная формулировка понятия ОРХП видится нам наиболее удачной с точки зрения ее значимости для получения информации о преступной деятельности, планирования оперативно-розыскных мероприятий, направленных на выявление и раскрытие преступлений.

Рассмотрим такой элемент ОРХП как личность мошенника в сфере компьютерной информации, являющийся одним из важных для организации инициативной работы по выявлению фактов мошенничества и его документированию.

Полагаем, что среди различных точек зрения на характерные черты личности типичного мошенника наиболее ценной представляется позиция Д.В. Ермоловича и С.В. Широких, которые, среди прочих социально-психологических признаков их личности, указывают следующие:

1. Глубокие познания в различных областях человеческой деятельности. Чаще всего это знания в области психологии, поведенческих особенностей и поступков в типичных жизненных ситуациях. Они помогают создать условия для совершения преступного деяния, например: размещение ссылок на файлы вредоносного программного обеспечения в комментариях к объявлениям о продаже различных товаров с предложением обмена.

2. Определяющий мотив преступления – корысть. Соотнося данную характеристику с примерным возрастом типичного интернет–мошенника (примерно 17-35 лет, причем основной процент будет приходиться на период с 18 до 24 лет [5]), можно заключить, что типичный интернет-мошенник – учащийся ВУЗа или учреждения среднего профессионального обучения, не работающий и, возможно, находящийся на иждивении родителей или других лиц. Что в свою очередь определяет его доход от преступной деятельности как основной.

3. Хорошие коммуникативные качества, наблюдательность, изобретательность, неординарность поступков, специфические формы общения, способы и приемы решения поставленных задач. Именно эти качества позволяют разрабатывать и использовать методики по удержанию внимания жертвы в фокусе преступного деяния и достижения желаемого результата. [6]

К перечисленным признакам необходимо дополнить познания в области информационных технологий. Их уровень определяет вид и способ компьютерного мошенничества, на которых специализируется преступник.

Одним из примеров характерных признаков личности мошенника в сфере компьютерной информации может послужить случай, произошедший в г. Барнаул. У гражданина М. был зарегистрированный на его имя профиль на сайте «Авито», в котором им размещались объявления о продаже различного рода специализированной техники для воспроизводства музыка (колонки, усилители, магнитофоны различных типов). М. имел большой опыт продаж такого рода техники, самостоятельно мог осуществить её ремонт и реставрацию, знал тонкости общения с потенциальными покупателями такого рода товаров. По новостному телеканалу он увидел репортаж о мошенничествах с использованием компьютерной информации и проблемах, возникающих при раскрытии подобного рода преступлений, что, его словам, подтолкнуло на совершение противоправного поступка. После этого используя абонентский номер сотового телефона, зарегистрированный на подставное лицо, он регистрирует профиль на сайте «Авито» под вымышленными данными. На этом профиле он размещает объявления о продаже различных систем усиления звука и активно предлагает указанный товар жителям других регионов, с целью минимизации количества заявлений обманутых граждан. Потерпевшие от преступной деятельности М. поясняли, что товары, выставленные на сайте «Авито» указанным продавцом были хорошего качества и имели большую ценность для любителей, коллекционеров и профессионалов в музыкальной сфере. Продавец очень четко понимал тонкости в пересылке товара и потерпевшие до самого последнего момента не верили, что их попросту обманули, несмотря на то, что с момента предоплаты проходило большое количество времени, и не писали заявления в полицию. В ходе рассмотрения материалов проверки М. дал признательные показания по 5 фактам своей преступной деятельности.

Стоит отметить, что это далеко не полный перечень признаков, которыми обладает лицо, совершившее мошенничество в сфере компьютерной информации.

Список литературы

1. Алферов В.Ю. Правовые основы оперативно-розыскной деятельности / В.Ю. Алферов, А.И. Гришин, Н.И. Ильин ; под общ. ред. В.В. Степанова. – 3-е изд., испр. и доп. – Саратов : Саратовский социально-экономический институт (филиал) РЭУ им. Г.В. Плеханова, 2016. – 296 с.

2. Борин Б.В. Понятие, определение и значение оперативно-розыскной характеристики преступлений экономической направленности // Пробелы в российском законодательстве. 2014., №1. - https://cyberleninka.ru/article/n/ponyatie-opredelenie-i-znachenie-operativno-rozysknoy-harakteristiki-prestupleniy-ekonomicheskoy-napravlennosti (дата обращения: 05.12.2018).

3. Ожегов С.И. Словарь русского языка. М., 1981. С. 765.

4. Белкин Р.С. Криминалистика: проблемы сегодняшнего дня. М., 2001. – 240 с.

5. Кесарева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет. Канд. дисс. М., 2002, С. 103.

6. Ермолович Д. В., Широких С. В. Некоторые поисковые социально-психологические признаки личности мошенника // Юридическая Россия. – № 5 (47), 2008. - http://www.law.edu.ru/doc/document.asp?docID=1313226 (дата обращения 05.12.2018)

Б.В. Псарева,
к.ю.н., доцент кафедры уголовного процесса и криминалистики
Алтайский государственный университет, г. Барнаул

ЛИЧНОСТЬ ПРЕСТУПНИКА, СОВЕРШАЮЩЕГО ПРЕСТУПЛЕНИЯ С ПРИМЕНЕНИЕМ ИНФОРМАЦИОННО-КОММУНИКАТИВНЫХ ТЕХНОЛОГИЙ

Компьютерная преступность оказывает отрицательное влияние на развитие информационных отношений, причиняя при этом крупный ущерб гражданам, организациям и государству. По данным Генеральной прокуратуры РФ в период с января по октябрь 2018 году правоохранительные органы России зарегистрировали более 141000 преступлений (следствием завершено 35000 из них), совершенных при помощи информационно-коммуникационных технологий им в сфере компьютерной информации.[1]

Актуальными являются исследования личности киберпреступника [2, 3] в виду активного использования цифровых технологий. Кроме того, в настоящее время в России, в странах СНГ не всегда органы, ведущие борьбу с киберпреступлениями могут

похвастать наличием в достаточном количестве кадрами, что позволяет этой группе преступников чувствовать себя уверенно.

Следует иметь ввиду, что в российском законодательстве нет понятия «киберпреступление», есть понятие «преступление, совершенное с применением информационно-коммуникационных технологий». Употребляя в статье понятие «киберпрестуник», «хакер», «крэкер», мы будем иметь ввиду лиц, совершающих преступления с применением информационно-коммуникативных технологий.

Личность явление социально-психологическое, которое формируется благодаря проживанию человека в обществе. Наряду с понятием «личность» употребляется термин «индивидуальность». Понятие «индивидуальность» связано с духовными качествами человека и, в первую очередь, психическими явлениями, а именно психологическими свойствами личности. Определяющим свойством личности является, конечно, ее направленность. В основе направленности лежит система мотивов, отношение человека к обществу, самому себе, трудовой деятельности.

Рассуждая о самоконтроле и саморегуляции человека необходимо говорить о самопознании, что являет собой основу самооценки. Самопознание связано с уровнем притязаний человека.

Киберпреступник, с точки зрения психологии, это попытка самоутверждения, в первую очередь это касается несовершеннолетних и не только их.

В личностной системе ценностей киберпреступников первое место отводится личностным или групповым (клановым) эгоистическим ориентациям. Такая личность в первую очередь ставит «Я»-свободу, комфортные условия существования, материальные интересы, эгоистические устремления.[4, 292-293]

Наблюдается деформация правового и нравственного начала. Мотив, как правило, корыстный. Угрызения совести не мучают этих преступников. Исходя из социального расслоения общества, для них является незазорным позаимствовать материальные ценности у соотечественников, иностранных граждан, в своей стране, за рубежом.

Хакер в отличие от большинства других преступников не отличается физической активностью. Он при совершении преступления находится перед компьютером, как правило, в местах комфортного времяпрепровождения. Исходя из этого они, как правило, могут не ощущать страх быть обнаруженными. Это среда для социального раздвоения, как социальной игры, связанной со сменой ролей и декораций.[5, с.399]

В сознании прослеживается тенденция, что киберпреступник воспринимает себя отличным среди других, он творит, нежели разрушает. Это важный момент с точки зрения профилактики такого рода преступлений.

Нужно отметить, что хакер не всегда преступник одиночка. Наблюдается объединение их в преступные группировки, имеющие иногда транснациональный характер.[6, 87] Это, как правило, профессиональной тип преступника-хакера, который не работает в одиночку и готовит преступления очень тщательно.

Корыстный тип киберпреступника, например, фишинг преступник, это юный хакер непрофессионал (возраст до двадцати одного года), он использует уже готовые коды, разработанные специалистами, имеет достаточное количество неконтролируемого свободного времени, обладает завидным упорством в достижении цели.[7, 43]

Имеется такая разновидность преступников в их типологии личности, как преступники с психическими отклонениями. Таковые встречаются и среди хакеров. Речь идет о таком психическом расстройстве как сидром Аспергера. В СМИ появляется информация о том, что разрушен миф о гениальности рассматриваемой категории лиц. Суды признают их вменяемыми, но учитывают данное заболевание как смягчающий фактор при назначении наказания.[8]

Последнее время в нашей стране активизировался сексуальный тип киберпреступников. Они совершают такие преступления, как незаконное распространение порнографических материалов, нажива, корыстное начало для них не главное, они имеют цель на понуждение действий сексуального характера, развратные действия. Как показывает судебно- следственная практика города Барнаула чаще всего объектом посягательства у них являются несовершеннолетние. В этом случае речь может идти о насильственно-сексуальном типе преступника. Как и любой другой преступник сексуальной направленности сексуальный киберпреступник имеет низкую мораль, эгоистичен в достижении цели, любитель получать удовольствия. При наличии неопровержимых доказательств такие преступники идут на сотрудничество со следствием, признаются в содеянном.

Обобщенный портрет классического хакера-одиночки нарисовал А.Ю. Комиссаров (ЭКЦ МВД) [9]: чаще всего это лицо мужского пола от пятнадцати до сорока пяти лет (в России чаще всего до двадцати пяти) без уголовного прошлого, обладающее либо очень большим, либо, наоборот, очень маленьким опытом работы на компьютере. Почти всегда яркая личность, способная к принятию

ответственных решений и нетерпимая к насмешкам и потере социального статуса, трудоспособен, старателен.

На сегодняшний день в психологии применяются различные подходы к классификации лиц, совершающих преступления, которые вполне приемлены для характеристики личности киберпреступника. Наиболее серьезные попытки предпринимаются в нескольких аспектах: этиологическом, характерологическом, клиническом, социологическом, прогнозирования, смешанном (например, предрасположенность) и, поддерживаем точку зрения Н. Ахтырской, [10] седьмом аспекте – умственном. Психологическую характеристику лица, совершающего преступления с применением информационно-компьютерных технологий необходимо дополнить исследованием характеристики ума. Индивидуальность его проявляется в широте, глубине, самостоятельности, критичности, быстроте и гибкости.

Как показывает сложившаяся ситуация, в борьбе с рассматриваемыми преступлениями и их профилактики необходим серьезный междисциплинарный подход, в котором не последнее занимает юридическая психология. Требуется активизация научных психологических исследований в этой области.

Список литературы

1. Генеральная прокуратура составила портрет типичного российского хакера//vedomosti.ru›technology/news/2018/12/11/788967

2. Поляков В.В. Характеристика личности киберпреступников / В.В. Поляков, Н.В. Людкова // Теоретические и практические проблемы организации раскрытия и расследования преступлений: сб. мат. Всерос. науч. практ. конф. 22 апреля 2016 г.; - Хабаровск: ДВЮИ МВД России. - С. 250-255.

3. Поляков, В.В. Особенности личности компьютерных преступников / В.В. Поляков, Л.А. Попов // Известия Алтайского государственного университета. – 2018. –№ 6 (104). – С. 256-259.

4. Долгова А.И. Криминология /под ред. А.И.Долговой.- М.1997.292-293 с.

5. Кравченко А.И. Общая психология.- М., 2011. С.399

6. Евдокимов К.Н. Особенности личности преступника, свершающего неправомерный доступ к компьютерной информации/Сибирский юридический вестник- 2011. №1 С.87

7. Джеймс Л. Фишинг. Техника компьютерных преступлений/ пер. с англ.Р.В.Галицкого- М.:НТ Пресс, 2008. 43 с.

8. Русского хакера оправдали из –за аутизма//xakep.ru›2009/08/11/49152/

9. Комиссаров А.Ю.Криминалистическое исследование письменной речи с использованием ЭВМ:Дисс. … канд.юрид.наук. Москва, 2001. 225 с. РГБ ОД.61:01-12/596-8 Социальный и психологический портрет хакера//securitylab.ru›news/215317.php

10. Ахтырская Н. Психологический портрет киберпреступника//crime-research/ru

М.Е. Репин,
начальник смены дежурной части отдела полиции №5 Управления МВД России по г. Нижнему Новгороду

ЛИЧНОСТЬ IT-ПРЕСТУПНИКА КАК ЦЕНТРАЛЬНЫЙ ЭЛЕМЕНТ КРИМИНАЛИСТИЧЕСКОЙ ХАРАКТЕРИСТИКИ ПРЕСТУПНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Для всего мирового сообщества конца XX и начало XXI столетий характерным было стремительное и бурное развитие высоких технологий. Особенно ярко и отчетливо это стало ясно уже на пороге XXI века. Одной из основных движущих сил динамичного развития экономики и общества стала информация и IT-технологии. Но в рамках информатизации и глобализации общественных отношений, одновременно с прогрессом, наблюдается и рост преступной деятельности в сфере информационных технологий. Компьютерные преступления в России уже давно перестали быть редкостью. Ответственность за их совершение в Уголовный кодекс РФ введена довольно давно, но еще 10 лет назад таких деяний было совсем немного, уголовные дела носили единичный характер. Сейчас с каждым годом незаконных действий с использованием IT-оборудования становится все больше и больше. Об этом факте нам свидетельствует статистика, предоставленная ФКУ «ГИАЦ МВД России».

Статистические данные ГИАЦ МВД РФ о раскрываемости преступлений в сфере компьютерной информации [1]

Год	2013	2014	2015	2016	2017
Количество преступлений в сфере компьютерной информации	241	258	268	280	327
Общее количество зарегистрированных преступлений в год	2628,8 тыс.	2404,8 тыс.	2302,2 тыс.	2206,2 тыс.	2241,5 тыс.
Процентное соотношение	0,0009 %	0,0011 %	0,0012 %	0,0013 %	0,0014 %

За темпом развития информационных технологий очень сложно угнаться, особенно такой основательной структуре, как законодательная. Именно поэтому возникает масса особенностей преступлений в сфере информационных технологи. Вот лишь некоторые из них:

- трудоемкое доказательство вины какого-либо лица;
- усложненный поиск улик;
- отсутствие свидетелей;
- необходим большой багаж знаний;
- и т. д. [2]

Множество заявлений и сообщений не рассматривают из-за отсутствия состава преступления, который также неоднозначен. Преступники активно пользуются всеми слабостями, часто оставаясь в тени. Однако есть положительная тенденция на улучшение качества расследования и доказательства вины злоумышленников. Мы отчетливо понимаем, что стремительное и неуклонное развитие информационных технологий предполагает, с одной стороны, определенное качественное улучшение процессов и условий жизнедеятельности общества и его индивидов, а, с другой – совершенствование механизмов совершения IT-преступлений.

Преступники в IT-сфере с каждым днем становятся более информационно осведомленными, теоретически подготовленными и технологически оснащенными, повышая собственный уровень грамотности и профессионализма. Это, в свою очередь, способствует

развитию преступности в данной сфере, в том числе и транснациональной.

Данные проведенного социологического опроса показывают, что по количеству жертв от преступной деятельности в сфере информационных технологий Российская Федерация занимает одну из лидирующих позиций среди ведущих экономически развитых мировых стран [3, с. 12–13].

Личность преступника в сфере информационных технологий можно рассматривать в двух смыслах: узком и широком. В узком смысле – это лицо, которое совершило виновное противоправное деяние, предусмотренное главой 28 «Преступления против компьютерной информации» Уголовного Кодекса Российской Федерации:

– статья 272 УК РФ «Неправомерный доступ к компьютерной информации»;

– статья 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ»;

– статья 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»;

– статья 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» [4].

В современных условиях развития общественных отношений прослеживается устойчивая тенденция проникновения традиционных форм преступности в интеллектуально-информационное виртуальное пространство. Поэтому мы можем судить о том, что, в широком смысле, «IT-преступник» – это лицо, которое в процессе совершения действий преступной направленности использует современные информационные технологии. В настоящей статье мы более детально рассмотрим узкий подход в трактовке данного понятия.

Криминалистическую характеристику преступления составляют «взаимосвязанные и корреляционно зависимые элементы той или иной категории преступлений» [5, с. 27]. Рассматривая преступления в сфере информационных технологий, мы полагаем, что определяющим и ключевым элементом является личность «IT-преступника». Личность преступника связывает между собой два базисных элемента криминалистической характеристики преступной деятельности любого рода и вида – обстановку совершения преступления и способ.

Мы предприняли попытку исследования и анализа взаимосвязи личности информационного преступника, совершающего

преступления в сфере IT-технологий, со способом совершения преступной деятельности. Как известно, характеристика способа совершения преступления основывается на трех составляющих – «подготовка, совершение преступление и сокрытие следов» [6, с. 13]. Конкретный способ совершения преступной деятельности в рассматриваемой в настоящей статье сфере зависит от целого ряда личностных свойств и качеств «IT-преступника», от присущих ему компетенций, знаний, умений и навыков.

Создание, использование и распространение вредоносных компьютерных программ определенно и непосредственно зависит от уровня интеллекта преступника, его материального состояния (предполагает наличие информационно-технических приборов и средств) и ближайшего окружения (родственники, друзья, знакомые, коллеги). Использованию вредоносных программ предшествует их поиск, модификация уже имеющихся, создание уникальных разработок. Такая градация обусловлена пропорциональным ростом сложности выполняемой задачи. Очевидно, что модификация уже имеющихся вредоносных программ или создание своих уникальных разработок требует большего объема специальных знаний (например, знание языков программирования), чем поиск готовых программ.

Материальный аспект находит свое прямое отражение в возможности приобретать то или иное программное обеспечение или техническое устройство. Это, бесспорно, влияет на скорость доступа к различным информационным базам и данным (тоже самое можно сказать и о неправомерном доступе). Следует отметить, что для совершения большинства преступлений в сфере информационных технологий не требуется наличие какого-либо дорогостоящего оборудования и техники. В современных условиях развития общества в глобальной информационно-телекоммуникационной сети Интернет существует множество платных и бесплатных вредоносных программ, которые содержат необходимый для совершения преступных действий алгоритм операций.

Таким образом, способ совершения преступной деятельности в сфере информационных технологий напрямую и главным образом зависит от интеллектуальных аспектов личности правонарушителя и, в некоторой степени, его финансового благополучия и материального положения.

Далее мы рассмотрим обстановку совершения преступной деятельности в сфере IT-технологий. Как нам известно из теории криминалистической науки, обстановка является одним из

структурных элементов криминалистической характеристики преступления.

Так, Р.С. Белкин отмечал, что в содержание обстановки преступления помимо объектов внешней материальной обстановки, необходимо включать следующие элементы: «поведение участников события, обстоятельства, способствующие или препятствующие действиям этих участников, хронологическую составляющую события, психологические отношения, возникающие между участниками события» [7, с. 139]. По нашему мнению, такая широкая трактовка понятия обстановки сужает ее сущность в криминалистической характеристике преступлений в сфере информационных технологий.

Обстановка совершения преступной деятельности в сфере IT-технологий отличается своим стремительным развитием и динамичностью. Если мы рассмотрим обстановку совершения традиционного преступления (например, кража, мошенничество, дача взятки, превышение должностных полномочий и т.д.), то можем сказать, что преступник подстраивается под неё.

На наш взгляд, специфика и уникальность обстановки совершения преступных действий в сфере информационных технологий заключается в том, что она двояка. Так, например, В.В. Поляков отмечает, что «важным в обстановке является не только пространственный элемент, но и иная информационная обстановка с соответствующим порядком хранения, обработки, использования и защиты компьютерной информации» [8, с. 114]. С одной стороны, мы рассматриваем обстановку материального мира, а с другой – виртуального кибернетического пространства. Мы считаем, что во втором случае обстановку создает сам преступник. Речь не идет о непосредственном создании новой операционной системы.

Виртуальная обстановка – это система взаимодействующих процессов в операционной системе. Именно они характеризуют состояние работоспособности программного обеспечения, его распространение, уровень защиты и другие показатели. Такая обстановка создается определенной последовательностью действий лица и путем кодирования или алгоритмизации. Виртуальную обстановку можно условно разделить на обстановку в операционной системе преступника и обстановку в операционной системе потерпевшего. В первом случае преступник сам создает обстановку. От него зависит функционирование программного обеспечения, систем защиты и т.д. Во втором случае, он работает в уже имеющейся ситуации и модифицирует её с целью достижения преступного замысла. Например, преступник запускает анти – анитивирусный

вирус и нарушает работу защитного программного обеспечения в операционной системе потерпевшего.

Примерами таких программ могут быть вирусные «черви», троян, кейлоггеры, вирус-сканеры и т.д. Их создание может быть выражено не только в изготовлении и полной подготовке к работе, но и в чертеже схемы, на основе которой предполагается использовать вредоносные системы, а также в написании алгоритма, при введении которого наступит одно из последствий, указанное выше.

Так, гр. К. Е.П. понес наказание за создание специальной программы-спама, с помощью которого он взламывал страницы одной из социальных сетей. При этом настройки вредоносного спама были такими, что пользователи, зашедшие на «зараженную» страничку, тоже «приносили» в свой компьютер вирус. Таким образом, гр. К. Е.П. был привлечен не только за создание вредоносной программы, но и за ее использование и распространение [9].

Представленное нами определение и классификация позволяют сделать вывод о том, что обстановка совершения преступления в сфере компьютерной информации носит двойственный характер и имеет сложную структуру.

При совершении преступных действий в сфере информационных технологий отсутствует непосредственное взаимодействие между преступником и самим потерпевшим. Вследствие этого, личность потерпевшего отходит на второстепенный план.

Подводя итог, можно сказать, что личность «IT-преступника» занимает центральную часть криминалистической характеристики преступлений в сфере информационных технологий. Способ и виртуальная обстановка совершения таких преступлений носят зависимый характер от личности правонарушителя.

Список литературы

1. Главный информационно-аналитический центр МВД России [Электронный ресурс]: состояние преступности – статистика и аналитика. URL: https://xn--b1aew.xn--p1ai/mvd/structure1/Centri/Glavnij_informacionno_analiticheskij_cen (дата обращения: 20.10.2018).

2. Кошелева Е.Е., Афанасьев А.Ю., Репин М.Е. Некоторые особенности применения специальных знаний в выявлении коррупционных рисков уголовно-процессуального доказательственного права // Южно-уральские криминалистические чтения: сборник докладов международной научно-практической

конференции (под ред. Макаренко И.А.). Уфа, 2015. Выпуск 23. С. 85–89.

3. Афанасьев А.Ю., Репин М.Е. Уголовно-процессуальные и криминалистические особенности расследования киберпреступлений // Криминалистическое обеспечение раскрытия и расследования преступлений: Материалы X Всероссийского научно-практического круглого стола (Ставрополь, 26 февраля 2016 г.). Том 1. Ставрополь, 2016. С. 12–13.

4. Уголовный кодекс Российской федерации от 13.06.2006 № 63-ФЗ // Российская газета. 2006. 25 июня.

5. Каневский Л.Л. Дискуссионные проблемы сущности типовой криминалистической характеристики преступлений и ее использования в процессе расследования // Вестник криминалистики. М., 2002. С. 27.

6. Колесниченко А.Н. Общие положение методики расследования отдельных видов преступлений. Харьков, 1965. С. 13.

7. Белкин Р.С. Собирание, исследование и оценка доказательств: сущность и методы. М., 1966. С. 139.

8. Поляков В.В. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики / В.В. Поляков // Известия Алтайского государственного университета. – 2013. – № 2. – С. 114 - 116.

9. Обстановка совершения преступлений в сфере компьютерной информации как элемент криминалистической характеристики // Право. Барнаул, 2012. С. 114.

10. Юрсовет: Преступления в сфере компьютерной информации [Электронный ресурс]. URL: http://juresovet.ru/prestupleniya-sfere-kompyuternoj-informacii/ (дата обращения: 22.11.2018).

С.С. Симонова,
к.ю.н., доцент кафедры уголовно-правовых дисциплин
Волгоградский институт управления – филиал РАНХиГС

ОСНОВНЫЕ НАПРАВЛЕНИЯ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

В современном мире киберпреступность является одной из самых распространенных форм транснациональной преступности. Быстрое развитие киберпространства привело к относительно новому типу преступлений, а именно к киберпреступности, которая превосходит как временные, так и пространственные условия для совершения традиционных преступлений. Киберпреступления являются наиболее сложными для раскрытия, поскольку преступная деятельность с использованием информационных технологий зачастую не ограничивается пределами одного государства, что удлиняет обнаружение подобных преступлений во времени и усложняет их расследование.

Широкое распространение киберпреступлений также связано со способом их совершения – по сути, преступник имеет возможность находясь в любом месте, всего за несколько секунд распространить вредоносную программу, заразить вирусом базы данных или иным способом совершить преступление, посягающее на информационную безопасность любого объекта, включая как личность, общество, так и государство в целом.

Вышеизложенные проблемы обеспечения информационной безопасности имеют значение не только в мировом, но и в национальном масштабе. Так, в России только за 2017 год было зафиксировано около 20 тысяч компьютерных преступлений.

Проблема предупреждения преступлений, совершаемых с использованием информационных технологий, является особо актуальной в период перехода Российской Федерации к цифровой экономике. Появление криптовалюты, все более широкое использование технологии блокчейн, цифровизация экономики и бизнеса – все эти новшества порождают качественно новый вид правоотношений, ведь любые отношения, происходящие в обществе между индивидами и имеющие юридические последствия, можно назвать правовыми отношениями. Следовательно, так называемые информационные правоотношения нуждаются в особой охране от

преступных посягательств в рамках требований принципов российского уголовного права.

Следует отметить, что профилактика преступлений, совершаемых с использованием информационных технологий, обладает определенной спецификой. Это связано, в первую очередь, с объектами киберпреступлений, поскольку информационная безопасность является особым объектом уголовно-правовой охраны. Доктрина информационной безопасности 2016 года определяет информационную безопасность Российской Федерации как «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства» [1].

В связи с вышеизложенным представляется важным исследовать основные направления профилактики преступлений, совершаемых с использованием информационных технологий.

В юридической науке существует ряд методологических подходов к определению понятия профилактики (предупреждения) преступлений. К примеру, в рамках системного подхода предупреждение преступности определяется как многоуровневая система государственных (правоохранительных) и общественных мер, направленных на выявление и устранение (ослабление) или нейтрализацию причин и условий преступности, оказание предупредительного воздействия на лиц с противоправным поведением [2, с. 14-43].

Комплексный подход рассматривает профилактическую, предупредительную деятельность как одно из средств социального регулирования общественных отношений в целях устранения причин преступности; как взаимодействие мер экономико-социального, воспитательно-педагогического, организационного и правового характера; как сочетание различных уровней предупреждения преступлений. В соответствии с данным подходом предупреждение преступности буквально означает предохранение людей, общества, государства от преступлений. Предупреждение преступности представляет собой сложный комплекс разнообразных мер, предупреждающих воздействие на все, что порождает, воспроизводит социально негативное явление, определяет его неблагоприятные тенденции, качественно-количественные характеристики. [3, с. 772] На

наш взгляд, использование комплексного подхода к профилактике преступлений, которые совершаются с использованием информационных технологий, является наиболее верным, поскольку сама проблема киберпреступности является сложной и многоаспектной.

Одним из важнейших направлений профилактики преступлений, совершаемых с использованием информационных технологий, является международное сотрудничество. Как было установлено нами выше, преступления с использованием информационных технологий представляют угрозу не просто отдельным странам, а в целом мировому сообществу. Следовательно, особо эффективным способом профилактики киберпреступности является интенсивное сотрудничество на международном уровне. При этом, Интерпол и Европол являются наиболее распространенными субъектами как профилактики преступлений, совершаемых с использованием информационных технологий, так и расследования указанных преступлений в рамках так называемого международного полицейского сотрудничества.

Следующим важным направлением профилактики преступлений, совершаемых с использованием информационных технологий, является виктимологическая профилактика. Большое количество киберпреступлений совершается именно из-за низкого уровня компьютерной грамотности значительной части населения. В связи с этим в рамках виктимологической профилактики необходимо повышать компьютерную грамотность населения, причем у различных возрастных категорий должны быть особо освещены различные аспекты информационной безопасности. Так, у людей старшего поколения вызывают определенные сложности вопросы, касающиеся использования безопасного контента, хранения персональных данных и недопущение их незаконного распространения. Пользователям среднего возраста необходимо иметь представление об угрозах, связанных с использованием электронных платежных систем, а также при использовании технологии блокчейн, облачных хранилищ и криптовалюты.

Особую сложность представляет профилактика преступлений, которые совершаются с использованием информационных технологий несовершеннолетними или в отношении несовершеннолетних. Важно отметить, что проблема обеспечения информационной безопасности несовершеннолетних, должна решаться в двух аспектах. Во-первых, речь идет о профилактике преступлений несовершеннолетних, совершаемых в сети Интернет, а во-вторых, о виктимологической профилактике среди детей и подростков, направленной на

минимизацию риска стать жертвой преступления, связанного с использованием информационных технологий.

Рассмотрим основные виды рисков, которым подвержены дети и подростки в сети Интернет:

1) Контентные риски (материалы, содержащие насилие, агрессию, эротику и порнографию, нецензурную лексику, информацию, разжигающую расовую ненависть, пропаганду анорексии и булимии, суицида, азартных игр, наркотических веществ).

2) Коммуникационные риски (незаконные контакты по типу груминга, киберпреследования, кибербуллинг).

3) Электронные риски (хищение персональной информации, вирусные атаки при помощи вирусов, червей и «троянских коней», онлайн-мошенничество, спам-атака, шпионские программы).

4) Потребительские риски (злоупотребление в Интернете правами потребителя, приобретение товара низкого качества, различные поделки, контрафактная и фальсифицированная продукция, потеря денежных средств без приобретения товара или услуги, хищение персональной информации с целью кибермошенничества) [4].

Представляется, что для снижения уровня указанных рисков и минимизации их пагубного воздействия на несовершеннолетних необходимо расширить правовое регулирование вопросов, касающихся обеспечения информационной безопасности детей и подростков. В первую очередь, такие меры должны быть приняты на законодательном уровне. В России в последнее время наметились некоторые положительные сдвиги в данном направлении. Так, в октябре 2018 года был принят Законопроект заместителя Председателя ГД РФ И.А. Яровой, направленный на защиту жизни детей от так называемых колумбайн-сообществ, оперативное выявление преступников, вовлекающих несовершеннолетних в противоправную деятельность, опасную для их жизни и профилактику угроз безопасности жизни детей. Данный законопроект разработан в рамках деятельности Экспертного совета по вопросам совершенствования законодательства в сфере обеспечения безопасности детей и формирования доброжелательной и комфортной среды для их жизни и развития и поддержан Роскомнадзором, МВД, Следственным комитетом, Генеральной прокуратурой, Министерством связи и массовых коммуникаций, Министерством просвещения.

Законопроектом предусмотрена фиксация следов удаленного контента для того, чтобы «сохранить эти материалы для правоохранителей в качестве источника для формирования

доказательной базы и обоснованного решения о привлечении виновных лиц к уголовной ответственности. По словам Ирины Яровой, «правоприменительная практика подтверждает эффективность ранее принятых мер по защите жизни здоровья детей от вовлечения в «группы смерти» и от любых других сообществ, распространяющих преступный контент. Только в 2017 году на основании изменений в закон, которые были инициированы нами, было заведено 200 уголовных дел, заблокировано 1,5 тысячи «групп смерти» и несколько сотен тысяч публикаций» [5].

В целях реализации основных положений Концепции информационной безопасности детей Министерством связи и массовых коммуникаций в феврале 2018 года утвержден План мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы. [6] План стал продолжением работы по реализации Концепции информационной безопасности детей, утверждённой Правительством Российской Федерации в 2015 году в рамках Национальной стратегии действий в интересах детей на 2012-2017 годы. Целью Плана является создание условий формирования безопасной информационной среды для детей, в частности:

- проведение мониторингов, посредством которых выявить возможности улучшения сопровождения детей в информационном пространстве,
- разработка методических рекомендаций, которые позволят снять дефицит информации у образовательных учреждений и снизить нагрузку на исполнение работ по обеспечению информационной безопасности образовательной среды,
- обмен опытом между законодателями и педагогическими работниками в рамках конференции и парламентских слушаний,
- проведение мероприятий по обучению детей основам информационной безопасности и популяризации этих знаний среди взрослых и в первую очередь родителей и педагогов.

Также планируется проведение ежегодных круглых столов, образовательных и просветительских форумов, различных конкурсов, премий и других мероприятий, в том числе конкурса социальной рекламы на тему информационной безопасности детей, конференции по формированию детского информационного пространства «Сетевичок», Всероссийского конкурса социальной рекламы на тему информационной безопасности детей. В реализации плана задействованы исполнительные органы государственной власти -

Минпросвещения России, Минкомсвязи России, Роспотребнадзор, Минздрав России и другие.

На наш взгляд, реализация мероприятий, указанных в Плане, может способствовать повышению уровня защиты несовершеннолетних от рисков, связанных с использованием сети Интернет, и следовательно, стать эффективным направлением виктимологической профилактики киберпреступлений, совершаемых в отношении несовершеннолетних.

Говоря о нормативно-правовых мерах профилактики преступлений, совершаемых с использованием информационных технологий, следует особо отметить, что в действующем законодательстве отсутствуют организационно-правовые меры защиты детей от информации, которая содержится в играх и игрушках. Как следствие, дети оказываются не защищены от того вреда, который наносится их нравственному, психическому развитию в компьютерных и онлайн-играх, содержащих насилие, жестокость, призывы к суициду и порнографию. В Концепции информационной безопасности детей, утвержденной распоряжением Правительства РФ от 2 декабря 2015 г. № 2471-р, информационная безопасность детей определена как защита ребенка от дестабилизирующего воздействия информационной продукции и создания условий информационной среды для позитивной социализации и индивидуализации, оптимального социального, личностного, познавательного и физического развития, сохранения психического и психологического здоровья и благополучия, а также формирования позитивного мировосприятия [7].

Однако Концепция не является нормативно-правовым актом, обязательным к применению, а носит лишь декларативный, рекомендательный характер и содержит общие положения, основные принципы, приоритетные задачи государственной политики по обеспечению информационной безопасности несовершеннолетних.

Таким образом, современная нормативно-правовая система обеспечения информационной безопасности несовершеннолетних не в полной мере соответствует фактическим рискам и угрозам, возникающим в связи с развитием цифровых технологий и увеличением объема противоправного контента, который влечет рост киберпреступности и снижение уровня психического здоровья детей и подростков. [8, с. 21]

Говоря о профилактике киберпеступлений, следует учитывать и такой важный аспект, как криминологическая характеристика личности преступника. Лица, совершающие преступления с

использованием информационных технологий, безусловно, сами досконально их знают. Как правило, специальные знания, используемые преступниками при совершении киберпреступлений, позволяют им умело скрыть следы преступления, что значительно осложняет дальнейшее расследование. Практически все преступления, связанные с использованием информационных технологий, совершаются мужчинами. Так, все киберпреступления в период с 2010 по 2015 гг. были совершены только лицами мужского пола. Среди лиц, совершающих киберпреступления, велика доля молодежи и несовершеннолетних. Это связано, в первую очередь, с практически неконтролируемом доступом подростков к сети Интернет, а также с освоением компьютера с раннего возраста. За последнее время число несовершеннолетних пользователей Интернет резко возросло. Согласно статистике, в настоящее время в России насчитывается от 8 до 10 млн. интернет-пользователей в возрасте до 14 лет. При этом две трети детей выходят в Интернет самостоятельно, без присмотра родителей и педагогов. [9, с. 2] Зачастую хакеры объединяются в преступные группы, что придает совершаемым им преступлениям повышенную общественную опасность, причем как на внутригосударственном, так и на международном уровне.

Таким образом, нами были рассмотрены основные направления профилактики преступлений, которые совершаются с использованием информационных технологий - развитие международное сотрудничество, совершенствование нормативно-правового регулирования, конкретизация мер виктимологической профилактики в зависимости от возрастных особенностей потенциальных жертв киберпреступлений. На наш взгляд, только комплексное использование указанных профилактических мер может стать эффективным способом предупреждения преступлений, совершаемых с использованием информационных технологий.

Список литературы

1. Доктрина информационной безопасности Российской Федерации (утв. Указом Президента Российской Федерации от 5 декабря 2016 г. N № 646) / "Российская газета". - 2016. - 6 декабря.

2. Кобзарь И.А. Организационные и правовые основы предупреждения преступности несовершеннолетних период. дис…д-ра юрид. наук. М. - 2002. - 408 с.

3. Российская юридическая энциклопедия. М.: Издательский дом ИНФРА-М. - 1999. - 1110 с.

4. Меликова Н.Д. Влияние Интернета на психику людей // Universum: Психология и образование: электрон. научн. журн. 2015. № 11-12(20). URL: http://7universum.com/ru/psy/archive/item/2822 (дата обращения: 25.11.2018).

5. Госдума приняла в I чтении законопроект Яровой, защищающий детей от вовлечения в преступное сообщество и опасные группы / Официальный сайт И.А. Яровой. Электронный ресурс: режим доступа: http://xn--80ad9ah8ee.xn--p1ai/news/16453.html (дата обращения 25.11.2018).

6. Приказ Минкомсвязи России «Об утверждении плана мероприятий по реализации Концепции информационной безопасности детей на 2018-2020 годы» / Официальный сайт Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. 25 апреля 2018 г. Электронный ресурс: режим доступа: https://minsvyaz.ru/ru/documents/5994/ (дата обращения 06.11.2018).

7. Распоряжение Правительства РФ от 02.12.2015 N 2471-р «Об утверждении Концепции информационной безопасности детей» / "Собрание законодательства РФ", 07.12.2015, N 49, ст. 7055.

8. Гольтяпина И.Ю. Законодательство России в области обеспечения информационной безопасности детей // Эпоха науки. - 2017. - № 12.

9. Роина (Завалишина) О.В., Постоева Е.С., Загуменных Н.А. Обеспечение информационной безопасности обучающихся // Научный журнал КубГАУ. - 2017. - № 129 (05).

Н.В. Спесивов,
к.ю.н., доцент кафедры уголовного процесса
Саратовская государственная юридическая академия, г. Саратов

ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ СОВЕРШЕНСТВОВАНИЯ ПРАВОВОГО РЕГУЛИРОВАНИЯ ПРИМЕНЕНИЯ НАУЧНО-ТЕХНИЧЕСКИХ СРЕДСТВ В УГОЛОВНОМ ПРОЦЕССЕ

В настоящее время, в связи с динамичным развитием науки и техники, нельзя игнорировать вопросы, которые возникают в правовом поле при применении результатов технических средств в уголовном

судопроизводстве. Действительно, преимущество применения новейших технологий при фиксации доказательственной информации является неоспоримым, а возникающие в данной сфере проблемы заслуживают повышенного внимания.

Отдельными авторами отмечается необходимость замены используемого в УПК РФ термина «технические средства» (например, в ст. 166) на «научно-технические», что будет наиболее точно отражать их природу, а также внести в УПК РФ отдельную статью, посвященную их применению в процессе доказывания [7, С. 12-13]. Соглашаясь с данной точкой зрения, полагаем, что содержание данной статьи должно включать в себя: во-первых, понятие рассматриваемого нами явления; во-вторых, цель использования (традиционная в рамках теории доказывания: собирание, проверка, оценка доказательств); в-третьих, перечень субъектов, имеющих право использовать полученные результаты в качестве доказательственной информации, а также процессуальный порядок их оформления. Кроме того, взяв за основу УПК Республики Казахстан, предлагаем также законодательно закрепить и критерии применения научно-технических средств, а именно: научная состоятельность, законность, этичность, достоверность, эффективность и безопасность [1, С. 43].

Второй вопрос, который хотелось бы отметить, касается статуса результатов, полученных при использовании научно-технических средств участниками уголовного процесса. Так, в ст.84 УПК РФ результаты использования технических средств обозначены законодателем как «носители информации», выступающие как способ средства фиксации сведений в документах. Кроме того, в ст. 166 УПК РФ данные результаты обозначены законодателем лишь в качестве приложения к протоколу, что говорит об отсутствии самостоятельного доказательственного значения результатов применения научно-технических средств.

Таким образом, нельзя не заметить, что в самом УПК РФ содержатся существенные противоречия, которые касаются их процессуального статуса: в ст. 166 - это приложения к протоколу; в ст. 84 – это «документы», «носители информации», а исходя из смысла ст. 189 УПК РФ их вообще можно рассматривать в качестве вещественных доказательств. Отсюда некоторые авторы называют результаты применения научно-технических средств самостоятельными доказательствами, другие считают их лишь приложениями к протоколу, третьи – просто «документами» [5, С.51-52]. Данное положение вещей вызывает трудности и на практике, заставляя участников уголовного процесса пользоваться различными

ухищрениями с целью признания результатов применения технических средств как самостоятельных доказательств по делу. Полагаем, что законодательное закрепление вышеуказанного положения будет способствовать как разрешению практических проблем, так и положит конец научных спорам по данному вопросу, устранив существующие на сегодняшний день противоречия в нормах закона.

Важной проблемой использования электронных доказательств является то, что в век информационных технологий, когда большинство информации зафиксирована на любых электронных носителях, УПК РФ (ст. ст. 164, 166) обязывает следователя составлять протокол и переписывать информацию в электронном виде, переписывать увиденное в видеозаписях. Нередко следователю нужно осмотреть и описать гигабайты информации, что отнимает у него огромное количество времени. Необходимость оптимизировать деятельность следователя по собиранию доказательств в электронной форме очевидна. Следует согласиться с мнением ученых, что основным направлением оптимизации уголовного судопроизводства в условиях информационного общества должно быть создание электронного документооборота и электронного правосудия [2, С. 95-101], [3, С. 16-17]. Но на наш взгляд это нескорая перспектива. Уже сейчас возможно предусмотреть свободу выбора способов фиксации хода и результатов следственных и иных процессуальных действий, оставив в качестве одного из таковых письменный протокол.

Третий вопрос: сам перечень технических средств, который может использоваться в уголовном процессе. Если в ст. 84 данный перечень является открытым, то ст. 166 УПК РФ приводит его вполне исчерпывающим: «стенографирование, фотографирование, киносъемка, аудио- и видеозапись». На некорректность данной нормы обращалось внимание многих авторов (Р.С. Белкин, В.И. Гончаренко, С.А. Шейфер) [4, С.71-77].

Действительно, наука развивается, и мы не можем исключать возможность появления новых научно-технических средств, а значит необходимо и в уголовно-процессуальном законе оставить его открытым, во всех нормах, где имеется упоминание о научно-технических средствах, указав «и иные» в конце такого перечисления.

Проблема четвертая: кто вправе использовать научно-технические (технические) средства в доказывании по уголовным делам? Исходя из анализа норм УПК РФ, видим, что в качестве субъектов применения могут быть названы лица как процессуального (например, следователь, прокурор), так и непроцессуального статуса.

В качестве примера в отношении последних можно привести норму ч. 5 ст. 241 УПК, где указано, что лица, присутствующие в открытом судебном заседании, вправе вести аудиозапись и письменную запись, а с разрешения председательствующего - проводить фотографирование, видеозапись и (или) киносъемку. Однако некоторые авторы считают, что круг данных субъектов должен быть четко очерчен законом: следователь, дознаватель, прокурор, специалист, эксперт, защитник, оперативный работник.

Следует заметить, что немало научных статей в настоящий момент посвящено именно исследованию условий, при которых результаты оперативно-розыскной деятельности при доказывании по уголовным делам могут использоваться в качестве реальных доказательств. И, несмотря на норму ст. 89 УПК РФ о том, что данные доказательства должны соответствовать общим требованиям (допустимость, достоверность, относимость), на практике при их использовании возникает немало проблем. Например, А.Е. Федюнин, Сластенов В.В. отмечают, что использование данных доказательств, факт получения которых не подкреплен свидетельскими показаниями, в суде, как правило, ведет к утрате их доказательственного значения[6, С. 3-7].

Другая проблема: получение доказательств оперативно-розыскных мероприятий, полученных с помощью технических средств, ненадлежащими субъектами. Так, если в ст. 1, ст. 6 ФЗ «Об оперативно-розыскной деятельности» в качестве таковых названы должностные лица оперативных подразделений государственных органов, уполномоченных на то данным Федеральным законом, то на практике часто возникают ситуации необходимости их получения потерпевшими. Соответственно, согласно нормам закона, они признаются недопустимыми. Считаем целесообразным, внести в рассматриваемый Федеральный закон изменения, согласно которым результаты оперативно-розыскной деятельности, полученные с использованием технических средств потерпевшими будут являться допустимыми при соответствующем контроле со стороны оперативных работников.

На основании вышеизложенных аргументов и предложений считаем, что на сегодняшний день требуется более детальное нормативно-правовое регулирование использования результатов научно-технических средств в доказывании по уголовным делам, основанное на всестороннем изучении доктринальных разработок ученых-правоведов.

Список литературы

1. Еникеев З.Д. Механизм уголовного преследования. Уфа: Изд-во БГУ, 2004. С. 43.
2. Качалова О.В., Цветков Ю.А. Электронное уголовное дело - инструмент модернизации уголовного судопроизводства // Российское правосудие. 2015. N 2. С. 95 - 101.
3. Пастухов П.С. Модернизация уголовно-процессуального доказывания в условиях информационного общества: дис. ... д-ра юрид. наук. М., 2015. С. 16 - 17.
4. Тарасов М.А. О некоторых проблемах правового регулирования применения технических средств в уголовном судопроизводстве // Вестник Южно-Уральского государственного университета, 2009. № 40. С. 71-77.
5. Тертышник В.М., Слинько С.В. Теория доказательств. Харьков: Арсис. С. 51-52.
6. Федюнин А.Е., Сластенов В.В. Взаимодействие оперативных и следственных подразделений правоохранительных органов при использовании оперативно-значимой информации в доказывании по уголовным делам // Проблемы правоохранительной деятельности. 2011. № 1. С. 3-7.
7. Цомая С.Д. Правовое регулирование и доказательственное значение применения научно-технических средств в уголовном судопроизводстве: автореф. дис. ... канд. юрид. наук. М., 2007. С. 12-13.

Н.В. Тыдыкова,
кандидат юридических наук, доцент кафедры уголовного права и криминологии
Алтайский государственный университет, г. Барнаул

НЕКОТОРЫЕ ВОПРОСЫ УГОЛОВНО-ПРАВОВОЙ ХАРАКТЕРИСТИКИ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья 274.1 УК РФ об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации является абсолютно новой для действующего

уголовного законодательства, так как была введена Федеральным законом от 26.07.2017 N 194-ФЗ. Поэтому некоторые понятия, используемые при ее формулировании, требуют уяснения.

Непосредственным объектом составов, предусмотренных ст. 274.1 УК РФ, является безопасность критической информационной инфраструктуры Российской Федерации.

Статья 2 Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» дает понятие критической информационной инфраструктуры и предлагает понимать под ней объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов. Определение нельзя признать удачным, так как оно отсылает к другому понятию - объекты критической информационной инфраструктуры. Оно раскрыто в этой же статье. Под ними предлагается понимать информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры. И это определение не вносит ясности, так как требует уяснения еще одного понятия. Субъекты критической информационной инфраструктуры - это государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Таким образом, уяснение понятия критической информационной инфраструктуры возможно только на основе двух других понятий. Это обстоятельство позволяет дать негативную оценку техники такого определения. А в качестве рекомендации по совершенствованию законодательства в этой области можно предложить формулировать более полное определение критической информационной инфраструктуры, которое бы включало все необходимые признаки.

В России на основании Приказа ФСТЭК России от 06.12.2017 N 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» ведется реестр значимых объектов критической информационной инфраструктуры. Поэтому вопрос о рассматриваемом составе может возникнуть лишь после того, как соответствующий объект в установленном законом порядке прошел процедуру установления соответствия критериям значимости и показателям их значений и ему была присвоена соответствующая категория значимости. В настоящее время формирование такого реестра в РФ только началось.

Предметом преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, является компьютерные программы или иная компьютерная информация, заведомо предназначенные для неправомерного воздействия на объекты критической информационной инфраструктуры.

Думается, что к таким программам или информации можно относить как те, которые предназначены только для неправомерного воздействия на объекты критической информационной инфраструктуры, так и те, которые могут быть использованы в том числе и для других целей. В литературе отмечается, что функциональная направленность вредоносной программы, т.е. ее предназначение именно для посягательств на соответствующие объекты, может быть установлена только в случае уникальности средств и технологий программной защиты объектов критической информационной инфраструктуры [1]. Представляется, что такое ограничение из смысла статьи с необходимостью не вытекает, а установление назначения в каждом конкретном случае должно производиться с учетом всех обстоятельств. Поэтому, если по конкретному делу будет установлено, что соответствующая компьютерная программа или иная компьютерная информация создавалась, распространялась или использовалась именно для неправомерного воздействия на объекты критической информационной инфраструктуры (хотя по своим характеристикам могла быть использована и в иных целях тоже), квалификация по рассматриваемому составу не исключается.

По конструкции объективной стороны состав является формальным, так как последствия находятся за рамками состава. Предметом составов, закрепленных в частях 2 и 3 анализируемой статьи, является охраняемая компьютерная информация,

содержащаяся в критической информационной инфраструктуре Российской Федерации.

Составы, закрепленные в этих частях статьи, являются материальными. Для признания их оконченными необходимо установить наступление вреда критической информационной инфраструктуре Российской Федерации. Если такового не наступило, но установлено, что виновный действовал именно с таким умыслом, то содеянное следует квалифицировать как покушение на соответствующее преступление [2].

Часть 5 ст. 274.1 УК РФ предусматривает такой квалифицирующий признак, как тяжкие последствия. Так как ни объем вреда, ни содержание тяжких последствий не раскрыто (например, в примечании к статье), то эти признаки следует считать оценочными.

Субъект данного преступления общий, то есть физическое вменяемое лицо, достигшее возраста 16 лет. Субъектом ч. 3 ст. 274.1 УК РФ может быть как общий, так и специальный - в части соблюдения правил эксплуатации соответствующих средств, систем и сетей.

Вина в составе, предусмотренном ч. 1 рассматриваемой статьи, предполагает прямой умысел, что вытекает из указания на заведомость, в составах, закрепленных в частях 2 и 3 статьи, возможен как прямой, так и косвенный умысел. Состав части 3 статьи также может быть совершен и по неосторожности. Цель в составе, указанном в ч.1 ст. 274.1 УК РФ - неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, в том числе, уничтожение, блокирование, модификация, копирование информации, нейтрализации средств защиты указанной информации. В составах, предусмотренных частями 2 и 3 ст. 274.1 УК РФ, специально не указана. Мотив значения не имеет, может быть представлен как корыстью, местью, так и желанием продемонстрировать свои навыки умения.

Нетрудно заметить, что состав преступления, предусмотренный ст. 274.1 УК РФ, объединяет в себе признаки составов, предусмотренных статьями 272-274 УК РФ, и является специальным относительно них. Некоторые исследователи даже отмечают, что в связи с этим новый состав объединил в себе и все сложности, свойственные тем составам [3]. Однако, вместе с тем, существует и наработанная практика квалификации по ним. Например, «Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в

сфере компьютерной информации», утвержденные Генпрокуратурой России (документ не был опубликован) содержат определения некоторых понятий и другие важные для правильной и единообразной квалификации положения, которые могут быть использованы и при квалификации рассмотренного нового состава.

Таким образом, состав преступления, предусматривающий ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, в настоящее время не имеет наработанной правоприменительной практики, так как является новым, а формирование реестра значимых объектов критической информационной инфраструктуры Российской Федерации только началось.

Список литературы

1. Решетников А.Ю., Русскевич Е.А. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) // Законы России: опыт, анализ, практика. 2018. N 2. С. 51 - 55.

2. Решетников А.Ю., Русскевич Е.А. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации // Уголовное право. 2018. N 2. С. 86 - 95.

3. Новичков В.Е., Пыхтин И.Г. Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. – 2018. - №2 (73). – С. 25-29.

А.А. Фадеев,
помощник прокурора Индустриального района г. Барнаула, аспирант Университет прокуратуры РФ

ВНЕСУДЕБНОЕ ОГРАНИЧЕНИЕ ДОСТУПА К ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ КАК ОДИН ИЗ СПОСОБОВ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ ЭКСТРЕМИСТСКОЙ НАПРАВЛЕННОСТИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

Деятельность по противодействию экстремизму непосредственно связана с защитой интересов общества и государства, в связи с чем принимаемые уполномоченными органами решения вызывают повышенный общественный интерес. При неверном либо ненадлежащем применении норм действующего законодательства Российской Федерации действия правоохранительных органов могут спровоцировать неблагоприятные социальные последствия.

Так, согласно п. 27 Стратегии противодействия экстремизму в Российской Федерации до 2025 года, утвержденной Президентом РФ 28.11.2014, среди основных направлений государственной политики по противодействию экстремизму является осуществление мониторинга средств массовой информации и информационно-телекоммуникационных сетей, включая «Интернет», в целях выявления фактов распространения идеологии экстремизма, экстремистских материалов и незамедлительного реагирования на них.

В современных условиях сеть Интернет является виртуальной средой и «неограниченной и бесплатной площадкой» для деятельности личностей экстремистской направленности. Ввиду подобной доступности сети Интернет указанные личности решают и реализацию поставленные «цели и задачи», в числе которых финансирование, подстрекательство к совершению преступлений экстремистской направленности. Расширение направлений применения мобильных платформ неизменно способствует увеличение новых угроз, появляются новые формы правонарушения и порядка их совершения [1].

В соответствии с п. 1 ст. 15.1 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» в целях ограничения доступа к сайтам в сети Интернет, содержащим информацию, распространение которой в Российской Федерации запрещено, создана единая автоматизированная информационная система «Единый реестр доменных имен, указателей

страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – Единый реестр).

Согласно п.п. 2 п. 5 ст. 15.1. указанного Закона одним из оснований для включения в Единый реестр является вступившее в законную силу решение суда о признании информации, распространяемой посредством сети Интернет», информацией, распространение которой в Российской Федерации запрещено.

Непосредственное ограничение доступа к интернет – ресурсам осуществляет Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций, в распоряжении которых имеются два механизма, позволяющих пресечь распространение запрещенной информации в сети Интернет: блокировка сайтов на основании решения суда и внесудебная блокировка сайтов на основании требований органов прокуратуры РФ [2].

Органы прокуратуры Алтайского края активно участвуют в формирования практики применения полномочий по внесудебному ограничению доступа к информации в сети Интернет, содержащей призывы к осуществлению экстремисткой деятельности, участию в массовых (публичных) мероприятиях, причем проводимых с нарушением установленного действующим законодательством Российской Федерации порядка.

К примеру, прокуратурой Индустриального района г. Барнаула только за 11 месяцев 2018 года в Руководителю управления Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Алтайскому краю и Республике Алтай направлено более 6 информаций, по результатам рассмотрения которых, информационные материалы в сфере экстремизма включены в Единый реестр в соответствии со ст. 15.1 вышеуказанного Закона.

Ранее выявление и принятие работниками органов прокуратуры РФ соответствующих мер в указанной сфере способствует раннему противодействию преступлениям экстремистской направленности. Своевременное ограничение доступа к сайтам, в том числе информации экстремистского содержания в сети Интерне», широкого круга лиц не позволяет заинтересованным лицам достичь поставленных целей, «напитать» указанных лиц экстремистскими идеями, побудить в них действия к совершению преступлений экстремистской направленности.

В целях совершенствования работы в этом направлении сотрудниками прокуратуры РФ постоянно осуществляют мониторинг сети Интернет с целью недопущения проявления экстремизма на поднадзорной территории.

Список литературы

1. Хохлов Ю.П. Противодействие международному экстремизму и терроризму: опыт Генеральной прокуратуры Российской Федерации // Прокурор. 2018. №3. С. 53-56.

2. Абрегов Т.А. Об особенностях надзорной деятельности по пресечению распространения материалов экстремистского характера в сети Интернет // Прокурор. 2016. № 4. С. 13-15.

Л.М. Фетищева,
кандидат юридических наук, преподаватель кафедры профессиональных дисциплин факультета внебюджетного образования
Пермский институт ФСИН, г. Пермь

К ВОПРОСУ ОБ УГОЛОВНО-ПРОЦЕССУАЛЬНОЙ ФОРМЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ИСПОЛЬЗУЕМЫХ ДЛЯ СОБИРАНИЯ, ПРОВЕРКИ И ОЦЕНКИ ДОКАЗАТЕЛЬСТВ

Правоохранительными органами особое внимание уделяется использования информационных технологий в процессе доказывания на стадии предварительного расследования. Одним из главных способов получения доказательств является проведение следственных действий, связанных с обнаружением, собиранием, фиксацией, проверкой и оценкой следователем представленной в электронном виде информации об элементах юридического состава преступления. Именно при проведении таких следственных мероприятий используются информационные технологии.

Вопросы, связанные с производством следственных действий с использованием информационных технологий (например, изъятие, копирование, хранение материальных носителей информации в электронной форме при обеспечении обязательного участия специалиста), были в УПК РФ фрагментарно решены. Вместе с тем в

настоящее время в отечественном законодательства и научной доктрине общепринятое понятие, признаки, критерии допустимости электронных доказательств отсутствуют. Возникающие на практике проблемы (одна из самых распространенных проблем - сомнение в авторстве документа, его подлинности или неизменности) решаются путем проведения компьютерно-технической экспертизы.

Однако, в уголовно-процессуальных нормах не прописаны конкретные способы удостоверения подлинности и неизменности электронных доказательств, а так же критерии допустимости таких доказательств. В связи с этим, изъятие электронных носителей информации является, с одной стороны, одним из самых сложных следственных действий, а с другой, в связи реальными условиями жизни одним из самых распространенных. Однако на сегодняшний день уже существуют как разработки ученых-процессуалистов, так и правоприменительные рекомендации от ученых-криминалистов. Электронным носителем информации является внутренний накопитель на жестком магнитном диске, оптические диски различных видов, магнитно-оптические диски, карты памяти различных форматов, USB флэш накопители, гибкие магнитные диски, интегральная микросхема памяти, оперативное запоминающее устройство ЭВМ, постоянное программируемое запоминающее устройство ЭВМ, оперативное запоминающее устройство периферийных устройств и иные носители. Из содержания статей 81, 81.1, 182, 183 УПК РФ вытекает, что понятием «электронный носитель информации» охватывается весь указанный выше перечень устройств. Соответственно производство их изъятия возможно как в форме обыска, так и в форме выемки. Подробная характеристика указанных следственных действий была дана нами в первой главе. Согласно части 9.1 статьи 182 УПК РФ при производстве обыска электронные носители информации в обязательном порядке изымаются с участием специалиста. Уголовно-процессуальный закон, формулируя правила об обязательном участии специалиста, подразумевает, что таковое обязательно и при производстве следственных действий в форме обыска или выемки, и при фиксации доказательственной информации, представленной в электронном виде [1, С. 4, 7-11]; причем, что не только при изъятии, но и при копировании информации, представленной в электронном виде, с различных источников внешней памяти.

Среди всех возможных методов изучения информации в электронном виде необходимо отметить особо интересные методы, а именно изучение информации о с мобильных и компьютерных устройств, находящихся в физической доступности у специалиста, а

так же с удаленных накопителей внешней памяти, файлов браузеров, отображающих интересы пользователя, данные о временной и постоянной географической локации, текстовых и голосовых сообщений, отправленных с помощью различных мессенджеров.

С развитием технических средств особенно необычной представляется возможность снятия отпечатков пальцев и других физиологических данных пользователя, полученных со смарт-часов и мобильных телефонов. Кроме того, в настоящее время, помимо проведения таких мероприятий, есть возможность системного анализа полученной совокупности информации, например, ее сопоставления по времени и географическому местоположению для определения причастности к тому или иному преступлению.

На практике достаточно актуальной является тема изъятия различных устройств, которые своим прямым назначением не имеют запись, хранение и воспроизведение информации, хотя содержат в себе некий «электронный носитель информации» (чаще всего, это карты памяти различных форматов или MP3 плееры, которые, в первую очередь, используются для воспроизведения аудио-файлов, мобильные телефоны, цифровые фотоаппараты, различные мобильные игровые консоли). Так как данный «электронный носитель информации» может содержать доказательственную информацию, представленную в электронном виде, то изымается все устройство, в котором он содержится. Оно приобщается к делу в качестве вещественного доказательства и подлежит исследованию экспертами.

В УПК РФ указано, что следственные действия в форме обыска, выемки, фиксации доказательственной информации, представленной в электронном виде, должны проводиться с обязательным участием специалиста, однако, реальные обстоятельства диктуют исключения, и не во всех случаях изъятие такой техники должно производиться с участием специалиста. Это можно объяснить тем, что в настоящее время практически любой пользователь ежедневно или даже ежечасно пользуется мобильными устройствами и, соответственно, самостоятельно проводит манипуляции с ними и информацией в них. Речь идет о мобильных телефонах, планшетах и смарт-часах, ввиду чего нам видится разумным предусмотреть возможность следователя или дознавателя самостоятельно, без участия специалиста, производить обыск и выемку таких простейших электронных носителей, особенно в случае угрозы утраты или повреждения доказательств.

Одним из важнейших следственных действий по уголовным делам с использованием информации, представленной в электронном

виде, является проведение компьютерно-технической судебной экспертизы (далее СКТЭ). В научной литературе выделяют значительное многообразие разновидности компьютерных экспертиз [2, С. 310 - 313]. Причем объектом исследования СКТЭ может являться как информация, содержащаяся на носителях, так и непосредственно ее носители, иные технические устройства обработки и передачи данных, программное обеспечение и сетевые ресурсы. Задачи, которые решаются СКТЭ, можно свести к следующим: определение технических характеристик, свойств компьютера и программного обеспечения; выявление свойств и характеристик сетевого ресурса; получение доступа к тем или иным данным, если таковой ограничен; установление изначального состояния сети, а также её компонентов; выявление обстоятельств, касающихся того, когда и какие сетевые устройства были добавлены или удалены; оценка общего состояния вычислительной сети на основе отображения информации о ней на сменных носителях (жесткие диски, флеш- накопитель и так далее). Разумеется, информацию, представленную в электронном виде, можно изменить посредством прикладного программного обеспечения как специализированного, так и общего характера, для чего имеется ряд разнообразных звуковых, графических, видео и текстовых редакторов. Существуют возможности несанкционированного копирования информации. И от профессионализма эксперта во многом зависит возможность проверки и установления факта модификации информации, представленной в электронном виде. Специалисты повсеместно используют различные методы и средства защиты электронной информации на накопителях внешней памяти, такие как электронная подпись и хеш- функцию. Затронув тему установления экспертами модификации информации, необходимо отметить, что на сегодняшний день такая модификация может быть достаточно просто выявлена специалистами, например, такие следы остаются на сервере госоргана, банка или другой организации после передачи или изменения информации, что особенно актуально для преступлений, совершаемых с помощью информационных технологий.

Другие процессуальные действия, направленные на получение доказательственной информации, представленной в электронном виде нужны в связи с необходимостью обнаружения информации, хранящейся на накопителе внешней памяти, удаленно подключенном к системному блоку и расположенном в физическом удалении от фактического места производства следственных действий, места нахождения органа, осуществляющего предварительное расследование и судебное разбирательство. Кроме физической удаленности объекта

производства следственных действий, возможны случаи, когда объектом следственного сайта выступает «неовеществленная информация», например, база данных организации, веб-сайт или облачное хранилище. Ввиду того, что база данных может быть технически защищена от изъятия программными средствами, веб-сайт может иметь хостинг за пределами Российской Федерации, то выемка или изъятие будет практически не выполнимым следственным действием, ввиду чего для получения доказательственно значимой информации будет достаточно их осмотра [3, С. 19].

В связи со сложностью Интернет - технологий у правоохранительных органов возникают проблемы с поиском и определением местонахождения преступников в глобальной сети. Для раскрытия преступных деяний, совершенных в данной сфере, первоначальным шагом проведения оперативно-розыскных мероприятий является определение адреса или местоположения, использованного преступником для совершения противоправных действий.

К сказанному надо добавить, что собирание доказательственной информации, представленной в электронном виде, осуществляется в стадии предварительного расследования и посредством иных процессуальных действий. Например, при таком способе получения доказательств по делу как направление следователем запросов, которые в соответствии со ст. 26 ФЗ «О банках и банковской деятельности» [4] и ст. 26 ФЗ «О национальной платежной системе»[5] должны согласовываться с руководителем следственного органа для получения сведений о движении денежных средств по виртуальным счетам клиентов.

При расследовании преступлений, совершенных с использованием информационных технологий и оставивших следы в информационной среде, важным способом получения доказательственной информации является направление организатору распространения информации в сети «Интернет» запроса о предоставлении как информации об абоненте (фамилия, имя, отчество, номер договора о предоставлении услуги доступа в сеть Интернет, фактический адрес и пр.), так и информации, касающейся содержания сообщений абонентов связи.

В результате изменения законодательства возможности органов публичного уголовного преследования по получению информации таким путем расширились. Так, операторы связи обязаны хранить на территории Российской Федерации[6, п.1. ст. 64]:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи - в течение трех лет с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей услугами связи, голосовую информацию, изображения, звуки, видео- и иные сообщения пользователей услугами связи - до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки» . Помимо этого операторы связи обязаны предоставить обозначенной информации уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность. Такая информация предоставляется либо на основании запроса следователя, согласованного с руководителем следственного органа, либо по запросу суда [6, п.1.1 ст. 64].

Организатор распространения информации в сети «Интернет» обязан хранить на территории Российской Федерации [7, п. 3 ст. 10.1]:

1) 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;

2) текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео- и иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки.

Любой способ документирования приемлем в случае, если он гарантирует сохранность и неизменяемость доказательственной информации, представленной в электронном виде в судебный орган, уполномоченный принимать решение по существу уголовно-правового спора, и возможность исследовать и оценить аутентичность этой информации и верифицировать ее. Думается, что в обозримом будущем информационные технологии и технические средства обработки, хранения и передачи информации сделают ненужными бумажные уголовно-процессуальные документы, то есть возможен и логичен переход на электронный документооборот. При этом необходимо отметить, что следственный осмотр «электронных носителей информации», сопровождающийся протоколированием записанной на них информации, целесообразен лишь в случаях угрозы потери информации, повреждения самого устройства как

первоисточника или непреодолимых препятствий для представления этой информации суду из первоисточника.

На наш взгляд, более адекватным средством фиксации действий участников оперативно-розыскного мероприятия или следственного действия была бы видеозапись, то есть электронный документ. Основное требование к носителю информации, представленной в электронном виде, состоит в том, чтобы при его исследовании можно было подтвердить, во-первых, законность проводимых следователем действий, во-вторых, достоверность сведений непосредственно о содержании следственного действия.

Такое же широкое распространение информационных технологий при сборе и оценке доказательств имеет место и в судебных стадиях уголовного процесса. Применительно к судебным стадиям уголовного процесса употребляется термин «электронное правосудие», который включает в себя электронный документооборот [8], а также способы осуществления правосудия с использованием информационных технологий, например, с использованием аудио- и видеопротоколирования, электронного архива и электронных исполнений решений . Однако уже в настоящее время информационная инновация - видеоконференц-связь не только получила должное нормативно-правовое регулирование, но и, как было обозначено выше, получила широкое применение на практике.

Имеющийся опыт допроса свидетеля в порядке ст. 278.1. УПК РФ, осуществляемый посредством видеоконференц-связи, дает основания для разработки аналогичного института в отношении специалистов и экспертов, допрос которых становится возможным, например, в форме видеозаключений, зафиксированных на электронных носителях информации [9, С. 33 - 35].

В связи с тем, что действующий УПК РФ называет только «показания специалиста», не упоминая при этом «допрос» или «консультацию» специалиста, ряд ученых указывает на то, что процессуальный статус специалиста зачастую сложно отграничить от роли сведущего свидетеля. В этом ключе можно рассуждать о необходимости распространения процессуального статуса свидетеля, в том числе и на специалиста, в ходе допроса которого, выясняются, например, вспомогательные нюансы будущего исследования эксперта. Сегодня сопровождаемый видеозаписью дистанционный допрос сведущего свидетеля приводит к созданию видеодокумента, по гносеологическим признакам близкого к заключению специалиста, т.е. к тому виду доказательств, который выделен из числа других видов по состязательному, а не по гносеологическому признаку и без четких

аспектов определенного уровня уникальности производимых интерпретаций.

Обозначенное выше предположение дает основание полагать, что возможность введения в уголовный процесс на судебной стадии формы экспертных видеозаключений, зафиксированных электронным способом на электронный носитель, будет существенно упрощать и расширять возможности исследования доказательств в суде, предоставляемые в настоящее время.

Правовая природа участия сведущих лиц в уголовном судопроизводстве посредством использования видеоконфенц-связи не всегда бывает очевидна для понимания. Например, возможность использования видеоконфенц-связи для допроса свидетеля в порядке ст. 278.1. УПК РФ в случае тяжелой болезни свидетеля, которая препятствует явке в очной форме на судебное заседание. Представляется необходимым, что при таких обстоятельствах при допросе судом рядом со свидетелем должен находиться лечащий врач или иной медицинский персонал [9, С. 33 - 35].

В этой ситуации возникает весьма логичный вопрос, кем будет являться сопровождающий допрос врач. УПК РФ не дает на него ответа, однако опыт нормативно-правового регулирования такого вопроса имеется в Республике Казахстан. Так, ч. 8 ст. 210 УПК Республики Казахстан (далее - УПК РК) устанавливает, что в случае наличия у допрашиваемого заболевания, препятствующего явке в судебное заседание, допрос такого допрашиваемого производится с разрешения врача и в его обязательном присутствии. При наличии в УПК РК такой нормы - статус врача в уголовном процессе тоже не указывается конкретно, при этом от мнения врача фактически зависит производство допроса, возможность исследования доказательств. А само такое заявление делается устно врачом с протоколированием в видеозаписи перед непосредственным началом допроса. Кроме того, интересной представляется норма ст. 213 УПК РК, которая предусматривает возможность проведения допроса в досудебном и судебном производстве посредством использования технических средств с использованием информационных технологий видеосвязи. Основаниями для проведения допроса в порядке ст. 213 УПК РК является наличие болезни, препятствующей проведению допроса, необходимость обеспечения безопасности допрашиваемого, иные причины невозможности явки в очной форме, например, удаленность фактического местоположения лица, которое необходимо допросить.

Еще одним интересным следственным действием с применением информационных технологий, закрепленным ст.217

УПК РК, является депонирование показаний. В соответствии с обозначенной нормой прокурор, подозреваемый или защитник вправе ходатайствовать о допросе следственным судьей свидетеля или потерпевшего, если имеются основания полагать, что более поздний допрос может оказаться невозможным в силу объективных причин (постоянное проживание за пределами Республики Казахстан, выезд за границу, тяжелое состояние здоровья, применение мер безопасности). Допрос производится следственным судьей в присутствии прокурора, подозреваемого, защитника, а в случаях необходимости и других участников процесса. Протокол судебного заседания, в котором зафиксированы депонированные следственным судьей показания допрашиваемого лица, подписывается судьей и секретарем судебного заседания.

Сегодня использование видеоконференц-связи предусмотрено ч. 6 ст. 35, ч. 4 ст. 240, ч. 6.1 ст. 241, ст. 278.1, ч. 1 ст. 293, ч. 2 ст. 389.12, ч. 8 ст. 389.13, ч. 2 и 2.1 ст. 399, ч. 2 ст. 401.13 УПК РФ. Но в части полноты правового регулирования привлечения в уголовный процесс видеоконференц-связи остаются проблемы, что, безусловно, определяет актуальность исследования обозначенной проблемы. Использование видеоконференц-связи возможно для подсудимого (осужденного), потерпевшего, свидетеля, выбор своего места пребывания при этом распространяется на представляющих их адвокатов, иных представителей. При этом видеоконференц-связь обеспечивает не только получение показаний участников судебного заседания, но и изложение ими своей позиции, заявление ходатайств и жалоб.

В соответствии с Определением Конституционного Суда РФ от 19.05.2009 №576-О-П положения ст. 125 УПК РФ обязывают суд обеспечить содержащемуся под стражей заявителю жалобы возможность путем непосредственного участия в заседании суда или путем использования систем видеоконференц-связи ознакомиться со всеми материалами рассматриваемого судом дела и довести до сведения суда свою позицию, если принимаемое судом решение связано с применением к заявителю мер, сопряженных с его уголовным преследованием, ограничением его свободы и личной неприкосновенности; в иных случаях лицу, отбывающему наказание в виде лишения свободы, обеспечивается возможность довести до суда свою позицию путем допуска к участию в деле его адвокатов и других представителей, а также иными предусмотренными законом способами.

Кроме использования видеоконференц-связи в целях реализации потребности в обеспечении в организации сеанса связи между судом, рассматривающим дело, и лицом, содержащимся под стражей, использование видеоконференц-связи служит обеспечению безопасности участников уголовного процесса. Использование видеоконференц-связи в обозначенных случаях было предусмотрено ч. 6.1. ст. 241 УПК РФ, внесенной Федеральным законом от 21.07.2014 №251-ФЗ.

Список литературы

1. Шаевич, А.А. Особенности использования специальных знаний в сфере компьютерных технологий при расследовании преступлений: дис. ... канд. юрид. наук. / Шаевич, Антон Александрович. - Иркутск, 2007. - С. 4, 7-11;

2. Карогодин, В.Н., Кастомаров, К.В. Некоторые проблемы судебной компьютерно-технической экспертизы / В.Н. Карогодин, К.В. Кастомаров // Актуальные проблемы уголовного процесса и криминалистики России и стран СНГ: материалы научно-практической конференции, посвященной 80-летию со дня рождения Ю.Д. Лившица. - Челябинск. - 2009. - С. 310 - 313.

3. Бикмиев, Р.Г., Бурганов, Р.С. Собирание электронных доказательств в уголовном судопроизводстве / Р.Г. Бикмиев, Р.С. Бурганов // Информационное право. - 2015. - № 3. - С. 19.

4. О банках и банковской деятельности : Федер. закон от 02.12.1990 № 395-1 (ред. от 31.12.2017) // Собр. законодательства Рос. Федерации. - 1996. - № 6, ст. 492; Рос. газета - 2018. - № 1. - 9 января.

5. О национальной платежной системе: Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 18.07.2017) : принят Гос. Думой Федер. Собр. Рос. Федерации 14 июня 2011 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 22 июня 2011 г. // Собр. законодательства Рос. Федерации. - 2011. - № 27, ст. 3872; 2017. - № 30, ст. 4456.

6. О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (ред. от 03.08.2018) // Российская газета, № 135, 10.07.2003,

7. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 25.11.2017) : принят Гос. Думой Федер. Собр. Рос. Федерации 08 июля 2006 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 14 июля 2006 г. // Собр. законодательства Рос. Федерации. - 2006. - № 31 (ч. I), ст. 3448; 2017. - № 48, ст. 7051.

8. Электронное правосудие предусматривает только КАС РФ // Петербургский правовой портал
9. Селина, Е.В. Проблемы использования средств видеоконференц-связи в уголовном судопроизводстве / Е.В. Селина // Администратор суда. - 2015. - №4. - С. 33 - 35.

Е.А. Чёрная,
старший следователь отдела ГСУ ГУ МВД России по Алтайскому краю, адъюнкт
Омская академия МВД России

ПРОБЛЕМЫ РАЗГРАНИЧЕНИЯ СТАТЕЙ 159 УК РФ И 159.6 УК РФ В КВАЛИФИКАЦИИ КОМПЬЮТЕРНОГО МОШЕННИЧЕСТВА

Виртуальный мир мошенников в сети Интернет, пожалуй, самый латентный пласт нашего общества, члены которого совершают вполне реальные преступления, представляющие особую опасность для практически каждого человека, который хоть раз использовал любой из существующих гаджетов для выхода в Интернет.

С каждым годом преступная среда в Интернете множится, развивается и не отстает от технического прогресса, а существующее в настоящее время многообразие типажей интернет-преступников служит подтверждением этому. Рассмотрим некоторые из них:

- Крэкеры - программисты, которые взламывают серверы, программы и их лицензионную защиту ради наживы и заработка;
- Фрикеры - специалисты, которые достигли самого высокого уровня взлома телефонных сетей;
- Скамеры - извлекают личную информацию, а затем вымогают денежные средства у жертвы;
- Кардеры - используют банковские счета и крадут средства при электронной оплате услуг;
- Фроды - создают социально-доверчивый сайт, через который и выманивают деньги у пользователей [1].

Кроме приведенных типажей существуют вирусописатели, вирмейкеры, крипторы и прочие разновидности хакеров, которые создают и распространяют вредоносные программы и приложения, взламывают и совершают кибер-атаки на компьютерные системы.

В связи с многообразием виртуального преступного мира возникают вопросы:

- под юрисдикциюкакой статьи Уголовного Кодекса попадает то или иное преступление, совершенное в виртуальном пространстве?

- какой вид преступной деятельности, совершаемой в сети Интернет, необходимо квалифицировать по статье – 159 УК РФ «Мошенничество», а какие по статье 159.6 УК РФ «Мошенничество в сфере компьютерной информации»?

- как в судебно-следственной практике в процессе квалификации и вменения наказания, решить проблему разграничения статей Уголовного Кодекса за мошенничество, совершаемое в сети Интернет?

Отвечая на первый поставленный нами вопрос, вспомним, что в 90-е годы в нашей стране преступления с использованием компьютера, а уж тем более преступления с выходом в Интернет, были явлением весьма редким. Но, уже в 1996 году законодатели поступили весьма прозорливо и предусмотрели в Уголовном кодексе РФ три статьи по компьютерным преступлениям, объединив их в главу 28 «Преступления в сфере компьютерной информации», а именно:

- ст. 272 «Незаконный доступ к компьютерной информации»;

- ст. 273 «Создание, применение и распространение вредоносных компьютерных программ»;

- ст. 274 «Нарушение норм эксплуатации средств хранения, обработки или передачи компьютерной информации» [2].

Стоит отметить, что статьи главы 28 УК РФ своей формулировкой довольно четко определяют суть преступной деятельности, ответственность за которые предусмотрена в данных статьях.

Следующий вопрос, касающийся статьи 159.6 «Мошенничество в сфере компьютерной информации», до сих пор вызывает неоднозначные высказывания представителей юриспруденции. С того момента, как российские граждане становились пользователями сети Интернет и, до того времени, когда в виртуальном пространстве «поселились» мошенники, прошло несколько лет. Но за эти годы стало очевидным, что законодательная база нуждается в дополнениях, касающихся ответственности за мошеннические махинации, распространившиеся и совершаемые в глобальной сети.

До внесения в Уголовный кодекс РФ изменений 2012 года, для вменения наказания за мошенничество, совершенное в сети Интернет применялась статья 159 «Мошенничество» совместно со статьей 272 УК РФ «Неправомерный доступ к компьютерной информации» [3],

что, возможно, не всегда полно и точно могло отражать степень вины совершенного интернет-преступления.

Изменения, принятые 29 ноября 2012 года Федеральным законом № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации» [4], и введение статьи 159.6 УК РФ «Мошенничество в сфере компьютерной информации», казалось бы, должныупростить ситуацию в системе правовой ответственности и снять проблему с вменением наказания за интернет-мошенничество. Однако, как показывает судебная практика, чуда не произошло.

Получив в арсенал статью 159.6 УК РФ, правоприменители обрели проблему разграничения данной статьи со статьей 159 УК РФ.

Формулировка статьи 159.6 УК включает в себя такие понятия, как «мошенничество» и «компьютерная информация». Правовая трактовка этих понятий дается в статье 159 УК РФ и в примечание 1 к статье 272 УК РФ соответственно, изкоторых следует:

- Мошенничество - есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием [5];

- Компьютерная информация- это сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [6].

Пытаясь разобраться в сути стоящей проблемы, рассмотрим указанные статьи по признакам состава преступления, приведенные в таблице 1.

Таблица 1

Признаки состава преступления	**Статья 159 УК РФ**	**Статья 159.6 УК РФ**
Объект преступления	Отношения собственности. Предмет – имущество и право на имущество	Отношения собственности. Предмет – имущество и право на имущество
Объективная сторона	Деяние – хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием.	Мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления,

		блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей
Субъект преступления	Вменяемое физическое лицо, достигшее 16 лет	Вменяемое физическое лицо, достигшее 16 лет
Субъективная сторона	Вина в виде прямого умысла и корыстная цель	Вина в виде прямого умысла и корыстная цель

Сопоставив основные признаки состава преступления, мы видим полное соответствие двух статей по трем признакам из четырех: объект, субъект и субъективная сторона. Объективной стороной, в рассматриваемых нами статьях, в обоих случаях является хищение чужого имущества или приобретение права на чужое имущество, также совпадает. Различия объективной стороны заключаются лишь в способе реализации мошенничества:

- в случае статьи 159 УК РФ - путем обмана или злоупотребления доверием;

- в случае статьи 159.6 УК РФ - путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей [5].

Подобные сходства ни могут не вызывать вопросы при квалификации нормы за мошенничество и мошенничество в сфере компьютерной информации, а также проблемы при разграничении статей 159 и 159.6 УК РФ.

За многие годы судебной практики издано большое количество юридическое литературы, разработаны программы разграничения преступлений и составлены алгоритмы их квалификации [6], на основе которых проводится практическое разграничение типичных

преступлений. В основе разграничений лежат признаки, характеризующие объект, субъект, объективную и субъективную стороны, а также комплексное разграничение преступлений. Но, порой, нечеткие формулировки обстоятельств дела, элементов и признаков состава преступлений, зачастую приводят к замешательству следователей, прокуроров, судей при его квалификации и создают трудности при разграничении смежных преступлений.

Судебная практика дел о мошенничестве и мошенничестве в сфере компьютерной информации также показывает отсутствие единого подхода к применению этих норм. Это объясняется тем, что в современном виртуальном пространстве мошенничество – динамично развивающееся преступление с множеством схем и способов, что влияет на трансформацию классического мошенничества в мошенничество, имеющее свои специфические черты и отличия. Смещение понятия мошенничества в интернет-мошенничество и создает трудности в разграничении компьютерных преступлений.

Так, например, мошенники, посредством использования специальных программ-генераторов паролей, взламывают электронные кошельки с целью хищения денежных средств; с той же целью завладевают пин-кодами банковских карт, создают интернет-магазины с несуществующими товарами, за которые в виде предоплаты получают деньги горе-покупателей. Мошенники создают фейковую информацию о предприятии для приема граждан на высокооплачиваемую работу. Аферисты, от желаемых трудоустроиться, получают копии документов, по которым на имя доверчивых пользователей мошенники оформляют кредит и т.д.

Данные примеры указывают на то, что мошеннические схемы реализации с «земли» перешли в Интернет, а денежный эквивалент теперь выражается не только в купюрах, но и приобрел электронный вид,

Мошеннику не обязательно использовать межличностное общение с жертвой, и расстояние в данном случае значение не имеет. При этом, даже осужденный и отбывающий наказание преступник, имея выход в Интернет, может совершать такого рода преступления.

Преступления, приведенные в примерах, классифицируются по статье 159 УК РФ, хотя и совершаются при помощи сети Интернет.

Преступления по статье 159.6 УК РФ также совершаются в сети Интернет, только при этом используется особый способ совершения преступления - ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи

компьютерной информации или информационно-телекоммуникационных сетей. Предметом преступления может выступает не только имущество, но и право на владение этим имуществом. Приведем примеры.

Гражданка П., путем модификации личных данных в базе клиентов ООО «С.», получила доступ к личной странице гражданки Л., которая являлась VIP-клиентом данной компании. От имени Л., гражданка П. электронно оформила заказ товара с экспресс-доставкой на свое имя, которым по получению завладела [7].

Вначале преступница мошенническими действиями получала право использовать чужой личный кабинет, а потом и завладела имуществом.

Гражданин Ф., ранее работая в одном из филиалов ОАО "ВымпелКом", путем обмана получил доступ к рабочему компьютеру офиса. Пользуясь навыками, полученными во время работы в должности специалиста обслуживания и продаж, а также известными ему персональными учетными данными произвел ввод 12 корректировок в программу, в результате чего перечислил 7080 руб. на баланс находящейся в его распоряжении СИМ-карты [8].

В обоих примерах для наказания применялась статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации».

Завершая вопрос разграничения статьи 159 УК РФ и статьи 159.6 УК РФ при квалификации преступления и указывая на тот факт, что приведенных примерах мошеннические действия совершались в сети Интернет, стоит обратиться к Постановлению Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате».

В пункте 20 данного Постановления законодатель поясняет, что «По смыслу статьи 159.6 УК РФ вмешательством в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей признается целенаправленное воздействие программных и (или) программно-аппаратных средств на серверы, средства вычислительной техники (компьютеры), в том числе переносные (портативные) - ноутбуки, планшетные компьютеры, смартфоны, снабженные соответствующим программным обеспечением, или на информационно-телекоммуникационные сети, которое нарушает установленный процесс обработки, хранения, передачи компьютерной информации, что позволяет виновному или иному лицу незаконно завладеть чужим имуществом или приобрести право на него»[9].

В пункте 21 окончательно разграничивает статью 159 и статью 159.6 УК РФ, поясняя «Если хищение чужого имущества или приобретение права на чужое имущество осуществляется путем распространения заведомо ложных сведений в информационно-телекоммуникационных сетях, включая сеть «Интернет» (например, создание поддельных сайтов благотворительных организаций, интернет-магазинов, использование электронной почты), то такое мошенничество следует квалифицировать по статье 159, а не 159.6 УК РФ» [9]. На наш взгляд, вводя в УК РФ статью 159.6 законодатель вкладывал в определение - «сфера компьютерной информации» более широкий смысл, нежели сейчас, спустя шесть лет с момента введения данной статьи, эта формулировка может вместить в свое определение, в сопоставлении с тем перечнем компьютерных преступлений, которые имеют место на сегодняшний день. Местоположение данной статьи определено в главе 21 УК РФ «Преступления против собственности».

Проводя анализ судебной практики, считаем, что вернее было бы размещение данной статьи в главе 28 УК РФ «Преступления в сфере компьютерной информации» с некоторыми изменением в названии действующей статьи «Мошенничество в сфере компьютерной информации» на «Хищение в сфере компьютерной информации».

Список литературы

1. Актуальные новости криптоиндустрии, блокчейн инноваций. URL: https://bitok.blog/category/news (Дата обращения 01.12.2018).

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 12.11.2018). Консультант-Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/(Дата обращения 01.12.2018).

3. Постановление Пленума Верховного Суда РФ от 27.12.07 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» URL: http://www.garant.ru/products/ipo/prime/doc/1685377 (Дата обращения 01.12.2018).

4. Федеральный закон "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации" от 29.11.2012 N 207-ФЗ. Консультант-Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_138322/ (Дата обращения 01.12.2018).

5. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 12.11.2018). Консультант-Плюс. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (Дата обращения 01.12.2018).

6. Бушуев Г. И. Разработка системы квалификации преступлений в сфере чрезвычайных ситуаций, в сб.: Проблемы безопасности при чрезвычайных ситуациях. Обзорная информация. М., ВИНИТИ, 1995. Вып. 7

7. Справка по изучению судебной практики по уголовным делам о мошенничестве (ст. ст. 159 - 159.6 УК РФ) Ульяновского областного суда. URL: http://uloblsud.ru/index.php?option=com_content&task=view&id=2984 (Дата обращения 01.12.2018).

8. Уголовное дело N 1-296/2015. URL: https://rospravosudie.com/court-kirovskij-rajonnyj-sud-g-astraxani-astraxanskaya-oblast-s/act-497082572. (Дата обращения 01.12.2018).

9. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате». ГАРАНТ.РУ: http://www.garant.ru/products/ipo/prime/doc/71723288/#ixzz5YsO3GPOZ (Дата обращения 01.12.2018).

А.В. Шебалин,
к.ю.н., доцент, заместитель начальника кафедры криминалистики
Барнаульский юридический институт МВД России, г. Барнаул

О.В. Кругликова,
к.ю.н., доцент, начальник кафедры криминалистики
Барнаульский юридический институт МВД России, г. Барнаул

К ВОПРОСУ ОБ ОРГАНИЗАЦИИ РАСКРЫТИЯ И РАССЛЕДОВАНИЯ МОШЕННИЧЕСТВ С ИСПОЛЬЗОВАНИЕМ ЭЛЕКТРОННЫХ СРЕДСТВ ПЛАТЕЖА НАЧАЛЬНИКОМ ОРГАНА ДОЗНАНИЯ

С расширением спектра предлагаемых услуг электронных платежных систем, увеличением оборота электронных денежных

средств, сращиванием платежных систем с банковскими услугами, а также увеличением их активных пользователей, наблюдается рост мошенничеств, связанных с использованием электронных средств платежа (ст. 159.3 УК России) [1]. Следует указать, что для мошенников электронные платежи являются удобным способом получения денежных средств от потерпевших, так как позволяют не вступать в непосредственный контакт с обманутым лицом. При этом изначальный способ передачи информации от преступника потерпевшему, как правило, осуществляется посредством мобильной связи. Активное использование преступниками и иными лицами электронных средств платежа при совершении мошеннических посягательств вызывает необходимость оказания пристального внимания вопросам организации раскрытия и расследования таких преступлений со стороны начальника органа дознания, как основного субъекта организации работы по этому направлению [2].

Необходимо отметить, что помимо организационных полномочий, которые начальник органа дознания может использовать для оптимизации работы в указанном направлении, с 30 декабря 2015 года, то есть с момента введения в состав УПК России статьи 40.2, он стал обладать еще и полномочиями процессуальными [3].

Итак, перейдем к рассмотрению тех действий, которые входят в обязательный перечень мероприятий, производимых с целью организации раскрытия и расследования мошенничеств с использованием средств электронных платежа, которые должны осуществляться начальником органа дознания.

Во-первых, при заступлении на суточное дежурство следует проводить обязательный инструктаж следственно-оперативной группы, указывая на специфику совершения, а также раскрытия и расследования рассматриваемых преступлений. Необходимо напомнить полномочия, обязанности каждого из участников следственно-оперативной группы в аспекте работы по мошенничествам с использованием электронных средств платежа.

Во-вторых, необходимо контролировать результаты работы следственно – оперативной группы по рассматриваемым преступлениям. Отчет о проделанной работе следственно-оперативной группы целесообразно принимать перед сдачей дежурства. При этом контроль следует осуществлять по следующим направлениям:

1) количество и качество изъятых в ходе осмотра места происшествия следов;

2) качество проведенного подворно-поквартирного обхода (зависит от количества опрошенных лиц проживающих (работающих) в непосредственной близости от места совершения преступления);

3) наличие образцов изъятых образцов для сравнительного исследования (зависит от изъятых в ходе осмотра места происшествия следов). Отпечатки пальцев и ладоней рук на дактилоскопические карты, отпечатки подошв обуви следует отбирать не только у преступников, но и у заявителей. Кроме того, целесообразно рекомендовать участковым уполномоченным полиции и оперативным уполномоченным подразделений уголовного розыска получать указанные образцы при отработке на причастность к совершению преступления лиц, ранее судимых за совершение аналогичных общественно опасных деяний и т.п.

В-третьих, в соответствии со ст. 40.2 УПК России начальник органа дознания при обнаружении неполноты собранного материала вправе давать указания о проведении проверочных действий на стадии возбуждения уголовного дела [4]. Оптимальной точкой контроля собранного следственно-оперативной группой материала по рассматриваемым преступлениям и, соответственно, изложения упомянутых указаний является, как уже говорилось, момент перед сдачей участниками следственно-оперативной группы дежурства. При этом составление проекта таких указаний, возможно, поручить руководителям служб, которые традиционно, наряду с начальником органа дознания, присутствуют при анализе материалов, собранных следственно-оперативной группой. К таковым руководителям служб относятся: руководители следственных органов, главы подразделений дознания, уголовного розыска, экспертов-криминалистов, подразделений по организации деятельности участковых уполномоченных полиции, заместители руководителя территориального органа внутренних дел по оперативной работе, охране общественного порядка. Каждый из них контролирует работу следственно-оперативной группы по своим направлениям: качество и полноту полученных объяснений и т.п. Если материал собран некачественно, то начальник органа дознания полномочен принять решение о проведении повторного комплекса мероприятий всеми членами следственно-оперативной группы, а если ненадлежащее качество работы присуще одному из участников следственно-оперативной группы, то возможно только его, адресное направление для исправления допущенных ошибок и недочетов в проделанной работе.

В-четвертых, после доработки материала, собранного следственно-оперативной группой, или поступления в орган внутренних дел заявления по почте (в этом случае, как правило, следственно-оперативная группа к работе по поступившему сообщению о преступлении не привлекается) при передаче материала в следственный отдел или отдел дознания необходимо изучить его на предмет полноты сбора, выявить, в случае наличия, неполноту и дать указания в соответствии со ст. 40.2 УПК России. Зачастую по таким материалам отсутствует протокол осмотра места происшествия. Это происходит в связи с тем, что участковые уполномоченные полиции, оперативные уполномоченные уголовного розыска получают подобное сообщение о преступлении для проверки на вторые-третьи сутки после его совершения.

В–пятых, если при работе по раскрытию и расследованию мошенничеств с использованием электронных средств платежа материальные следы изъяты в дежурные сутки, то в обязательном порядке должно быть вынесено постановление о назначении судебной экспертизы. В том случае, если отсутствуют образцы для сравнительного исследования или идентифицируемый объект, то требуется назначение, хотя бы, диагностической судебной экспертизы.

В-пятых, при осуществления контроля раскрытия и расследования мошенничеств с использованием электронных средств платежа, производство по которым осуществляется в форме дознания, начальник органа дознания вправе назначать и производить совещания о результатах деятельности специализированных следственно-оперативных групп, совещания по нераскрытым преступлениям подобного рода, давать указания дознавателю в порядке статьи 40.2 УПК России, изучать уголовные дела перед принятием решения о приостановлении или прекращении, изучать уголовного дела о мошенничествах с использованием электронных средств платежа перед направлением его прокурору для утверждения обвинительного акта. В этом случае, при наличии к тому оснований, начальник органа дознания имеет право возвратить уголовное дело дознавателю со своими письменными указаниями о производстве дополнительного дознания.

Таким образом, рассмотренные нами направления организации начальником органа дознания раскрытия и расследования мошенничеств с использованием электронных средств платежа позволят осуществлять уголовно-процессуальную деятельность по таким преступлениям с наименьшей потерей времени, сил и средств.

Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта №16-33-01160-ОГН.

Список литературы

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 12.11.2018) // СПС КонсультантПлюс.

2. Поляков, В.В. Осмотр места происшествия при предварительной проверке сообщений о компьютерных преступлениях. I. Организационные основы / В.В. Поляков, А.С. Никитин // Уголовно-процессуальные и криминалистические чтения на Алтае: проблемы противодействие киберпреступности уголовно-процессуальными, криминалистическими и оперативно-розыскными средствами / Сборник научных статей / отв. ред. С.И. Давыдов, В.В. Поляков. - Барнаул: Изд-во Алт. ун-та, 2017. – Вып. XIV.- С. 87-95.

3. Федеральный закон «О внесении изменений в Уголовно-процессуальный кодекс Российской Федерации в части уточнения полномочий начальника органа дознания и дознавателя» от 30.12.2015 № 440-ФЗ // СПС КонсультантПлюс.

4. Никитин, А.С. Некоторые вопросы, связанные с изъятием компьютерной информации в рамках доследственной проверки / А.С. Никитин, В.В. Поляков // Проблемы правовой и технической защиты информации. Выпуск IV / Сборник научных статей. - Барнаул: Изд-во Новый формат, 2016. – С. 254-259.

УГОЛОВНО-ПРОЦЕССУАЛЬНЫЕ
И КРИМИНАЛИСТИЧЕСКИЕ ЧТЕНИЯ
НА АЛТАЕ

ВЫПУСК XV

Проблемы и перспективы противодействия преступлениям, совершаемым с применением информационных технологий

Сборник научных статей

Статьи публикуются в авторской редакции и

Оформление обложки – Ю. Плетнёва

Подписано в печать 27.12.2018 г.
Объем 13,25 уч.-изд. л. Формат 60х84/16. Бумага офсетная.
Тираж 100 экз. Заказ № 580

227