Казанский инновационный университет имени В. Г. Тимирясова

Серия «Цифровая безопасность»

И. Р. БЕГИШЕВ
И. И. БИКЕЕВ

ПРЕСТУПЛЕНИЯ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

Казань ▪ КИУ ИЗДАТЕЛЬСТВО «ПОЗНАНИЕ» ▪ 2020

УДК 343.3/.7:004
ББК 67.408.135
Б37

Печатается по решению ученого совета и редакционно-издательского совета Казанского инновационного университета имени В. Г. Тимирясова в рамках реализации Дорожной карты развития цифрового университета «Цифровой океан»

Рецензенты:
Т. М. Лопатина, доктор юридических наук, профессор, заведующий кафедрой уголовного права и уголовного процесса ФГБОУ ВО «Смоленский государственный университет»;
М. А. Ефремова, доктор юридических наук, доцент, профессор кафедры уголовно-правовых дисциплин Казанского филиала ФГБОУ ВО «Российский государственный университет правосудия»

Бегишев, И. Р.
Б37 Преступления в сфере обращения цифровой информации / И. Р. Бегишев, И. И. Бикеев – Казань: Изд-во «Познание» Казанского инновационного университета, 2020. – 300 с. (Серия «Цифровая безопасность»).
ISBN 978-5-8399-0726-3

Монография представляет собой первое в России комплексное исследование феномена преступлений в сфере обращения цифровой информации. В ней рассмотрены вопросы уголовно-правовой природы преступлений в сфере компьютерной информации, предложены решения выявленных проблем ответственности за их совершение, внесены рекомендации по противодействию исследуемой категории преступлений, а также варианты устранения пробелов нормативного регулирования.

Будет полезна научным и педагогическим работникам, обучающимся разных уровней профессионального и дополнительного образования, слушателям специализированных учебных заведений, сотрудникам правоохранительных и судебных органов, разным категориям пользователей цифровой информации, а также всем интересующимся вопросами обеспечения цифровой безопасности.

УДК 343.3/.7:004
ББК 67.408.135

ISBN 978-5-8399-0726-3

О Г Л А В Л Е Н И Е

ВВЕДЕНИЕ

Стремительное развитие цифровизации буквально всех сторон жизни ставит перед человечеством, а значит и перед Россией, новые, все более масштабные задачи. Меняется технологический уклад, развитие робототехники и искусственного интеллекта ведет к трансформации производств и колоссальным сдвигам трудовых ресурсов. Уходят некоторые привычные и приходят новые, ранее неизвестные профессии. Стремительные изменения всего множат риски.

Люди становятся все более доступными для наблюдения и воздействия извне, а значит, и более уязвимыми и беззащитными. Нас с вами можно подслушивать, за нами можно подглядывать через наши собственные телефоны, ноутбуки, телевизоры, пылесосы, компьютеры и другие технические устройства. Читать наши сообщения и записи в наших же гаджетах. Отслеживать с помощью камер видеонаблюдения и другого оборудования наши перемещения, взаимодействия с другими людьми, даже считывать выражение лица. И в какой-то момент внезапно и драматично вторгнуться в нашу жизнь, используя полученную без надлежащего согласия информацию…

В связи со сказанным реализация права на частную жизнь становится очень проблематичной. Возникают вопросы иногда даже философского уровня. Готовы ли мы менять приватность на цифровой комфорт? Кому можно доверять: производителю операционной системы, производителю программного обеспечения, производителю оборудования? Или никому из них? Ведь каждый из

названных субъектов может делать тайные «закладки», с помощью которых способен будет управлять системой издалека.

Технология перешагнула этику. Хранилища данных продолжают расти дикими темпами. Нужно ли наложить ограничения на использование данных своих граждан? Или даже готовы ли мы к превентивному наказанию на основе поведенческих паттернов? Не к этому ли ведет развитие событий? Много возникает вопросов, на которые пока нет ответов.

Цифровизация различных процессов позволяет совершать общественно опасные деяния на удалении, создавать инструменты манипулирования и уходить от ответственности. Похищать информацию, уклоняться от уплаты налогов, создавать серые схемы расчетов, в том числе с использованием криптовалют, ставить под контроль процессы разных предприятий и органов власти: банков, производств, больниц, электростанций, министерств и т. д.

Новые термины «фейковые новости», «информационные войны», «информационные атаки» прочно вошли в нашу жизнь. Они тоже в числе прочего результат изменений цифровой действительности.

Наконец, в последние годы появился феномен кибертерроризма, способного атаковать объекты жизнеобеспечения и обороны страны и может привести к колоссальным жертвам и разрушениям. Ведь достаточно незаконно получить управление дамбой, самолетом, каким-либо опасным промышленным объектом и использовать это…

Преступления, посягающие на цифровую информацию либо совершающиеся с ее использованием, разнообразны, а их виды множатся в связи со стремительным развитием науки и техники, а также изобретательностью правонарушителей. Не допустить негативных последствий цифровизации, в то же время правильно ее регулировать – важная задача государства.

Тем более что остановить изменения, повернув прогресс назад, невозможно. Тот, кто попытается это сделать, проиграет в конкурентном соревновании. Нужно использовать преимущества идущих процессов.

Не случайно Президент Российской Федерации В. В. Путин в Послании Федеральному Собранию Российской Федерации 20 февраля 2019 г. говорил о том, что все наше законодательство нужно настроить на новую технологическую реальность, на создание правовой среды цифровой экономики. Данная книга как раз и направлена в числе прочего на решение названной задачи.

Хотя вопросы ответственности за преступления в сфере компьютерной информации разрабатываются в нашей стране и за рубежом уже несколько десятилетий, об их окончательном решении говорить не приходится. По отдельным вопросам данной проблематики существуют различные, порой противоположные точки зрения. В теории уголовного права пока нет однозначного понимания цифровой информации как предмета преступления, недостаточно учтено развитие терминологии в сфере ее обращения, существуют пробелы в уголовном законодательстве в части ответственности за новейшие высокотехнологичные деяния в данной сфере.

Опасность соответствующих преступлений обусловлена не только масштабами пагубных воздействий, например результатами посягательств на критически важные и потенциально опасные информационные инфраструктуры, но и ростом их количества. Так, в 1997 г. российскими органами внутренних дел было зарегистрировано лишь 23 преступления в сфере компьютерной информации, а в 2018 г. – уже 2 454[1]. Следует отметить, что приведенные данные не в полной мере соответствуют реальному положению дел в связи с чрезвычайно высокой латентностью указанных преступлений.

Уголовно-правовая наука должна отражать потребности времени, учитывать развитие и состояние научно-технического прогресса, что, на наш взгляд, в настоящее время не реализовано в достаточной мере при уголовно-правовом регулировании отношений в сфере

[1] См.: Статистика и аналитика // Официальный сайт МВД России. URL: https://mvd.ru/Deljatelnost/statistics (дата обращения: 15.09.2019).

обращения цифровой информации. Представляется также, что в уголовном праве отдельные виды цифровой действительности следует относить к объектам повышенной опасности, под которыми предлагается понимать «элементы объективного, возможного для изучения внешним наблюдателем, мира, которые в силу присущих им особых свойств способны с высокой степенью вероятности при неправильном обращении с ними или неправильном их осуществлении причинить существенный вред физическому состоянию людей и других ценностей либо создать реальные условия для причинения такого вреда и за неправильное обращение с которыми или неправильное осуществление которых установлена уголовная ответственность»[2].

Сказанное свидетельствует о необходимости и актуальности комплексного изучения понятия и видов преступлений в сфере обращения цифровой информации. Авторы данной монографии базировались на работах многих других специалистов. Например, проблемы исследования информации, в том числе компьютерной, в качестве предмета преступления и объекта уголовно-правовой охраны нашли отражение в диссертационных исследованиях Р. Г. Асланяна (2016), М. А. Зубовой (2008), В. В. Челнокова (2013), И. А. Юрченко (2000), С. А. Яшкова (2005) и др.

Уголовно-правовые, организационно-правовые и криминологические аспекты преступлений в сфере компьютерной информации изучались в кандидатских диссертациях Р. К. Ахметшина (2006), В. А. Бессонова (2000), С. Д. Бражника (2002), С. Ю. Бытко (2002), В. В. Воробьева (2000), М. С. Гаджиева (2004), Р. Р. Гайфутдинова (2017), С. И. Гутника (2017), М. Ю. Дворецкого (2001), Д. В. Добровольского (2006), Р. И. Дремлюги (2007), А. С. Егорышева (2004),

[2] Бикеев И. И. Материальные объекты повышенной опасности в российском уголовном праве: общие и специальные вопросы. Казань: Познание, 2007. С. 50.

А. А. Жмыхова (2003), У. В. Зининой (2007), Д. А. Зыкова (2002), А. Ж. Кабановой (2004), В. С. Карпова (2002), А. А. Комарова (2011), А. Н. Копырюлина (2007), С. С. Медведева (2008), С. С. Наумова (2001), О. М. Сафонова (2015), Т. Г. Смирновой (1998), С. Г. Спириной (2001), М. В. Старичкова (2006), А. В. Суслопарова (2010), С. И. Ушакова (2000), З. И. Хисамовой (2016), М. А. Хурум (2019), С. С. Шахрая (2010) и некоторых других исследователей.

Среди работ, направленных на исследование мер противодействия неправомерному доступу к компьютерной информации, отметим диссертационные исследования Р. М. Айсанова (2006), А. М. Доронина (2003), К. Н. Евдокимова (2006), Д. Г. Малышенко (2002), М. А. Простосердова (2016), И. А. Сало (2011), В. П. Числина (2004), А. Е. Шаркова (2004), Д. А. Ястребова (2005) и некоторых других ученых.

Исследованию уголовной ответственности за оборот вредоносных компьютерных программ и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей посвящены кандидатские исследования Н. В. Летелкина (2018), М. М. Малыковцева (2006), Е. А. Маслаковой (2008), А. Н. Ягудина (2012) и других исследователей.

Проблемы, возникающие в связи с совершением преступлений в сфере электронной информации, рассматривались в диссертациях А. В. Геллера (2006), А. И. Малярова (2008), В. П. Щепетильникова (2006) и др.

Отдельные проблемы установления и реализации ответственности за незаконный оборот специальных технических средств, предназначенных для негласного получения информации, исследовались в трудах С. Д. Петроченкова (2013) и других авторов.

Обеспечению информационной безопасности уголовно-правовыми средствами, противодействию информационному терроризму и информационным преступлениям посвящены кандидатские диссертации С. К. Бадамшина (2018), А. С. Изолитова (2008), Д. А. Кал-

мыкова (2005), Д. А. Ковлагиной (2016), Е. В. Красненковой (2006), А. В. Мнацаканян (2016), А. А. Шутовой (2017) и других ученых.

Изучению проблем киберпреступности, ее криминологически значимых аспектов, а также мер уголовно-правовой борьбы с ней адресованы кандидатские диссертации Т. Л. Тропиной (2005), И. Г. Чекунова (2013) и других авторов.

Также отметим, что противодействию преступлениям в сфере компьютерной информации и правовому обеспечению информационной безопасности посвящены докторские диссертационные исследования Л. А. Букалеровой (2006), В. Б. Вехова (2008), Ю. В. Гаврилина (2000), Н. Ш. Козаева (2016), Н. Н. Куняева (2010), Т. М. Лопатиной (2006), В. А. Мещерякова (2001), А. Л. Осипенко (2010), Т. А. Поляковой (2008), В. Г. Степанова-Егиянца (2016), А. Ю. Чупровой (2015), М. А. Ефремовой (2018) и других ученых.

В то же время особую значимость для решения поставленных в диссертации задач имеют труды ученых различных специальностей, в которых, в частности, освещались отдельные аспекты правового режима информации, информационной безопасности, защиты информации и информационной инфраструктуры. К числу таких авторов относятся Г. А. Атаманов, О. Я. Баев, Ю. М. Батурин, И. Л. Бачило, И. Ю. Богдановская, В. А. Герасименко, В. А. Голубев, В. М. Елин, А. К. Жарова, С. В. Зарубин, П. Д. Зегжда, Н. А. Зигура, С. В. Карташов, А. Г. Кибальник, П. У. Кузнецов, В. Н. Лопатин, Н. А. Лопашенко, А. В. Лукацкий, В. П. Малков, А. А. Малюк, А. В. Минбалеев, А. В. Морозов, В. Б. Наумов, С. А. Петренко, Т. А. Полякова, Е. Р. Россинская, Е. А. Русскевич, В. А. Садовничий, Е. С. Саломатина, С. В. Скрыль, Е. В. Старостина, А. А. Стрельцов, М. В. Талан, Э. В. Талапина, О. В. Танимов, А. М. Тарасов, А. А. Тедеев, Л. К. Терещенко, М. И. Третьяк, Р. М. Узденов, З. И. Хисамова, А. А. Хорев, В. Н. Черкасов, Г. И. Чечель, В. П. Шерстюк, А. Н. Яковлев и др.

Однако проведенные исследования, несмотря на их несомненную ценность, не решили многие вопросы, имеющие существенное значение для уголовного права и практики применения уголовного законодательства.

Теоретическую основу монографии составляют также и труды отечественных и зарубежных авторов по уголовному и информационному праву, криминологии, информационной безопасности и защите информации: О. Ю. Антонова, Р. М. Айсанова, Л. А. Букалеровой, С. Ю. Бытко, В. Б. Вехова, А. Г. Волеводза, А. А. Гребенькова, О. В. Григорьева, Н. Л. Денисова, Д. В. Добровольского, К. Н. Евдокимова, М. А. Ефремовой, У. В. Зининой, А. Ж. Кабановой, В. С. Карпова, Н. Ш. Козаева, О. Н. Крапивиной, Е. В. Красненковой, Н. Н. Куняева, С. П. Кушниренко, Т. М. Лопатиной, А. И. Малярова, Е. А. Маслаковой, С. С. Медведева, В. А. Мещерякова, А. В. Мнацаканян, С. Д. Петроченкова, Д. Прокиса, Е. А. Русскевича, Б. Скляра, В. Г. Степанова-Егиянца, Т. Л. Тропиной, А. Ю. Чупровой, Г. А. Шагинян, А. А. Шутовой, В. Н. Щепетильникова, З. И. Хисамовой, И. А. Юрченко, С. А. Яшкова и др.

Цель монографии – комплексное исследование феномена преступлений в сфере обращения цифровой информации. А это подразумевает рассмотрение вопросов уголовно-правовой природы и видов таких деяний, внесение предложений по решению выявленных проблем ответственности за их совершение, практических рекомендаций по противодействию исследуемой категории преступлений, а также выработку вариантов устранения пробелов нормативного регулирования.

Совместная разработка вопросов противодействия преступлениям в сфере обращения цифровой информации была начата авторами данной монографии в 2006 г. в Казанском инновационном университете имени В. Г. Тимирясова (тогда – Институте экономики, управления и права (г. Казань)). В настоящее время наши совместные исследования продолжаются и развиваются.

В монографии также учтены некоторые наработки Казанского инновационного университета, сделанные во время образовательного интенсива «Остров 10–22», прошедшего 10–22 июля 2019 г. в Москве в Сколковском институте науки и технологий, на котором команда университета успешно представила проекты цифрового развития нашего вуза и создания научно-образовательного центра мирового уровня.

В настоящее время у нас в вузе реализуется Дорожная карта развития цифрового университета «Цифровой океан». Ведь университеты призваны быть подлинными источниками океана знаний, заполняющими весь мир. Развивается сотрудничество по соответствующим направлениям с Агентством стратегических инициатив. И представленная вашему вниманию книга – звено в цепи названной дорожной карты, плод более чем 10-летней работы авторов. Она начинает серию книг Казанского инновационного университета «Цифровая безопасность».

В 2017 г. И. Р. Бегишев в Казанском (Приволжском) федеральном университете успешно защитил подготовленную под научным руководством И. И. Бикеева диссертацию на соискание ученой степени кандидата юридических наук на тему «Понятие и виды преступлений в сфере обращения цифровой информации». Указанная диссертация, а также другие работы соавторов в дополненном, переработанном и систематизированном виде легли в основу этой книги. Данное обстоятельство позволяет выйти на новый, более высокий и масштабный уровень разработки феномена цифровой преступности.

Мы надеемся, что в связи с использованием в работе значительного количества примеров и научно-популярного стиля изложения она будет полезна всем интересующимся вопросами обеспечения цифровой безопасности. Мы будем очень благодарны читателям за их суждения о мыслях, изложенных в книге, и предложениях о совершенствовании наших разработок.

ГЛАВА 1

УГОЛОВНО-ПРАВОВАЯ ПРИРОДА ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

§ 1.1. Понятие цифровой информации

Сегодня цифровая информация присутствует буквально повсюду. Без нее немыслимо функционирование и развитие всех без исключения сфер деятельности человека, включая такие, как промышленность, строительство, энергетика, медицина, образование, культура, безопасность, управление и т. д. Основное ее назначение состоит в удовлетворении потребностей граждан и других субъектов в общении и взаимодействии. Следует отметить, что развитие систем мобильной и спутниковой связи, информационно-телекоммуникационной сети Интернет, зарождение новых информационных технологий и иных форм телекоммуникаций значительно увеличили роль цифровой информации в формировании глобального информационного пространства. Цифровая информация представляет собой основу в организации современных информационных отношений[3].

[3] Бегишев И. Р. Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву // Академический юридический журнал. 2011. № 2. С. 47.

Понятие «цифровая информация» прочно вошло в нашу повседневную жизнь. Мы не можем себе представить нашу жизнь без таких реалий, как цифровое фото, цифровое видео, цифровое телевидение, цифровая связь, электронно-цифровая подпись, цифровой документ, цифровые технологии и т. д. Словосочетание «цифровая информация» прочно закрепилось в нашей памяти, так как относится ко всем вышеперечисленным объектам.

Кроме того, это понятие оказывает значительное воздействие на правоотношения, складывающиеся в сфере электронной коммерции. По мнению А. Ю. Чупровой, электронная коммерция – это использование сети Интернет для ведения деловых операций. Классической ее формой выступают осуществляемые в цифровой форме коммерческие операции и сделки между организациями и физическими лицами. Осуществляемые в цифровой форме операции означают любые деловые операции с использованием цифровых технологий[4].

Информационное общество вместе со всеми безграничными возможностями технологий диктует условия развития экономических отношений. Все чаще информация становится важным активом компаний, одним из основных ресурсов, обеспечивающих деятельность организации. В процессе развития информационных технологий происходит несанкционированный доступ к данным, который может причинить серьезный материальный ущерб отдельным заинтересованным лицам и крупным организациям[5].

---

[4] Чупрова А. Ю. Электронная коммерция как объект уголовно-правовой охраны // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2008. № 1. С. 98; Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. … д-ра юрид. наук. М., 2015. С. 45.

[5] Шутова А. А. Социальная обусловленность норм об уголовной ответственности за посягательства на экономическую информацию // Вестник Нижегородской правовой академии. 2015. № 4 (4). С. 73.

В силу своих специфических свойств информация является выгодным ресурсом, на который достаточно часто осуществляется непосредственное воздействие в противоправных целях. Учитывая ценность информации в современном мире, особое значение приобретают перспективы ее уголовно-правовой охраны, а также противодействие злоупотреблениям ею[6].

Современные возможности обращения цифровой информации порождают все новые виды преступлений, направленных на завладение и манипулирование ей.

До вступления в силу изменений в Уголовный кодекс Российской Федерации (далее – УК РФ[7]) в редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ[8] в российском законодательстве отсутствовало легальное определение компьютерной информации. Так, раньше в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ не давалось определения понятия компьютерной информации, а только говорилось о носителях, в которых эта информация циркулирует. Указанный вопрос не учтен также и в основном нормативном акте, регулирующем отношения в сфере обращения информации. Так, Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информаци-

[6] Шутова А. А. Особенности функциональной роли информации в конструкции отдельных составов преступлений // Материалы XIII Международной научно-практической конференции «Татищевские чтения: актуальные проблемы науки и практики», г. Тольятти, 21–24 апреля 2016 г.: в 5 т. / М-во образования и науки Самарской обл., мэрия г.о. Тольятти Самарской обл., Univ. degli studi di Brescia (Италия), Волжский ун-т им. В. Н. Татищева. Тольятти: Волжский ун-т им. В. Н. Татищева, 2016. С. 307.

[7] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

[8] См.: О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 420-ФЗ от 07 декабря 2011 г. // СЗ РФ. 2011. № 50. Ст. 7362.

онных технологиях и о защите информации»[9] не дает определения понятия компьютерной информации.

До конца 2011 г. в отечественном законодательстве не было определения компьютерной информации, что препятствовало нормальному развитию информационной индустрии. Так, Ю. А. Угланов отмечает, что в российском законодательстве до сих пор отсутствует четкий понятийный аппарат, касающийся информации и информационного обмена. Это дает, в свою очередь, возможность манипулировать понятиями, вводить в заблуждение суд и уходить от ответственности. Если рассматривать подробнее нормативно-правовые акты России, то видно явное расхождение в понятиях и отсутствие четких определений, особенно в научных понятиях и технических терминах в нормативно-правовых актах, ГОСТах и иной технической литературе[10].

Данная пробельность отмечена и В. А. Васильевым. Он указывает, что традиция постоянного внесения изменений в действующие нормативные акты характеризуется тем, что изменения запаздывают или решают проблему лишь частично, в результате чего в законодательстве множатся правовые коллизии[11].

Как нам представляется, в этих позициях есть серьезное рациональное зерно, требующее скорейшего решения и развития. К аналогичным выводам приходит Л. А. Букалерова, предлагающая систематизировать и унифицировать терминологию в сфере уголовно-правовой охраны информации, употребляемую в Граж-

---

[9] См.: Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 г. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

[10] Угланов Ю. А. Правовые и организационные вопросы борьбы с преступлениями в сфере компьютерной информации в Российской Федерации // Доклад на VII Международной конференции «Право и Интернет». URL: http://www.ifap.ru/pi/07 (дата обращения: 23.05.2019).

[11] Васильев В. А. Проблемы развития законодательства в сфере борьбы с киберпреступностью // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/articles/vasil06 (дата обращения: 23.05.2019).

данском и Уголовном кодексах[12]. Автор считает, что отсутствие систематизации норм, регулирующих всю совокупность охраняемой уголовным законом информации, отрицательно сказывается на процессе их применения[13].

Действующему уголовному законодательству свойственно отсутствие унифицированного подхода к оценке преступлений в IT-сфере, единства в используемом понятийном аппарате и, как следствие, внесение рассогласованных и бессистемных изменений, которые не дают ожидаемого результата[14]. Кроме того, несовершенство законодательства, регламентирующего вопросы внедрения и использования достижений научно-технического прогресса, кроется главным образом в отставании от развивающихся инновационных общественных отношений[15]. Вместе с тем общеправовой проблемой остается ведомственная разобщенность нормативно-правовой базы в подходах к правовому регулированию различных аспектов внедрения в жизнь результатов научно-технического прогресса[16].

---

[12] Букалерова Л. А. Особенности уголовно-правовой охраны информации как предмета хищений // Уголовно-правовая политика и проблемы противодействия современной преступности: сборник научных трудов / под ред. д. ю. н., проф. Н. А. Лопашенко. Саратов: Сателлит, 2006. С. 540.

[13] Букалерова Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: автореф. дис. … д-ра юрид. наук. М., 2007. С. 25.

[14] Хисамова З. И. О конструкции норм уголовного законодательства, предусматривающих ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий // Уголовная политика и культура противодействия преступности: материалы Междунар. науч.-практ. конф. 30 сент. 2016 г. Краснодар: Краснодарский университет МВД России, 2016. С. 347.

[15] Козаев Н. Ш. К вопросу о генезисе уголовного права в условиях научно-технического прогресса // Общество и право. 2012. № 2 (39). С. 117.

[16] Козаев Н. Ш. Несовершенство законодательной техники как негативный фактор развития уголовного законодательства в условиях научно-технического прогресса // Вестник СевКавГТИ. 2016. № 1 (24). С. 83.

В идеале правовое обеспечение должно работать на опережение на основе результатов научно обоснованного прогнозирования. Так, для уголовного права методологической базой традиционно является долгосрочное, среднесрочное и краткосрочное криминологическое прогнозирование. Но, несмотря на работу в этом направлении, на сегодняшний день не удается обеспечить даже мгновенную обратную связь, т.е. связь, при которой величина смещения двух факторов во времени не имеет практического значения. Данный феномен определяется постоянным ускорением научно-технического прогресса. К сожалению, приходится констатировать эффект «запаздывания» в уголовно-правовой сфере, хотя в последнее время и уголовный, и уголовно-процессуальный закон часто критикуют за часто вносимые изменения, видя в качестве причин этого не быстро меняющиеся общественные отношения, а несовершенство самих исходных текстов нормативных актов[17]. В условиях меняющихся общественных отношений, развития науки и усложнения техники уголовное право предстает в роли мощного механизма воздействия на те сферы общественной жизни, где инновационный процесс проявился в большей степени[18]. При этом законодатель, в свою очередь, должен постоянно находить точку равновесия между установлением запретов под угрозой наказания и позитивным стимулированием к созидательной деятельности[19].

В 2010 г. Правительство Российской Федерации внесло в Государственную Думу Федерального Собрания Российской Федерации

---

[17] Козаев Н. Ш. Влияние научно-технических достижений на генезис уголовного права // Общество и право. 2012. № 5 (42). С. 127.

[18] Козаев Н. Ш. Уголовная статистика как зеркало общественных отношений, обусловленных научно-техническим прогрессом // Научный вестник Омской академии МВД России. 2014. № 4 (25). С. 3.

[19] Козаев Н. Ш. Некоторые вопросы противодействия преступности, использующей достижения научно-технического прогресса // Вестник СевКавГТИ. 2015. № 4 (23). С. 104.

проект № 404613–5 Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации»[20].

Вскоре принятый Федеральный закон от 11 июля 2011 г. № 200-ФЗ[21] привел к единообразию положения законодательных актов России, затрагивающих данные вопросы. Эта мера обусловлена существенными изменениями понятийного аппарата, используемого законодательством Российской Федерации в сфере информационных технологий.

В то же время общепризнанного определения цифровой информации в правовой науке пока не выработано. Из смежных терминов наиболее часто используется термин «компьютерная информация».

Забегая вперед, следует отметить, что в примечании к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[22] законодатель разместил определение компьютерной информации[23].

---

[20] См.: О проекте Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации»: Распоряжение Правительства Российской Федерации № 1097-р от 30 июня 2010 г. // СЗ РФ. 2010. № 27. Ст. 3544.

[21] См.: О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации»: Федеральный закон № 200-ФЗ от 11 июля 2011 г. // СЗ РФ. 2011. № 29. Ст. 4291.

[22] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 420-ФЗ от 07 декабря 2011 г. // СЗ РФ. 2011. № 50. Ст. 7362.

[23] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

Представляется, что размещение определения термина «компьютерная информация» в примечании указанной статьи является верным, но в силу неточности и размытости оно требует более тщательного анализа и трактовки.

А. Ю. Чупрова справедливо считает, что указание на форму представления информации в примечании к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ диссонирует с положениями Закона «Об информации, информационных технологиях и о защите информации» и не учитывает направления развития информационных технологий. В английских и американских научных журналах уже появились сообщения о способах передачи информации с помощью света, т.е. в основу распространения информации могут быть положены световые, а не электрические сигналы[24].

Проведем исторический анализ определения компьютерной информации как предмета преступления.

В. Б. Вехов верно отметил, что отсутствие четкого уголовно-правового определения компьютерной информации, единого понимания ее сущности как предмета преступного посягательства значительно затрудняет выработку общей концепции борьбы с компьютерными преступлениями[25].

Такое положение дел привело к тому, что различные ученые трактуют понятие «компьютерная информация» по-разному. Например, В. А. Мещеряков под ней понимает информацию, представленную в специальном виде[26].

---

[24] Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 132.

[25] Вехов В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. 2004. № 4. С. 15.

[26] Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж: Изд-во Воронеж. гос. ун-та, 2002. С. 46.

Аналогичную точку зрения высказывает и М. В. Старичков[27], который под компьютерной информацией понимает зафиксированные на материальном носителе сведения, представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах.

В трудах других представителей уголовно-правовой науки содержатся и иные определения понятия «компьютерная информация». Так, Н. А. Зигура предлагает считать, что компьютерная информация – это сведения, представленные в электронно-цифровой форме на материальном носителе, создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации[28]. Однако представляется, что включение в определение компьютерной информации термина «создаваемые аппаратными и программными средствами фиксации, обработки и передачи информации» является неоправданным. Это связано с тем, что создание компьютерной информации средствами фиксации и передачи информации невозможно, так как они являются только дополнительными элементами любой информационной системы. В связи с этим более уместным было бы говорить об аппаратных средствах создания и обработки информации, т. е. компьютерах, а в общем смысле – об информационно-телекоммуникационных устройствах, которые, как правило, и создают компьютерную информацию.

Более того, Н. А. Сивицкая считает, что уголовно-правовой защите помимо собственно сведений должна подлежать инфор-

---

[27] Старичков М. В. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института МВД России. 2014. № 1. С. 20.

[28] Зигура Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. … канд. юрид. наук. Челябинск, 2010. С. 9.

мация в виде баз данных и программ[29]. Аналогичной позиции придерживается и Р.М. Айсанов[30].

В то же время определение понятия «компьютерная информация» должно быть основано, прежде всего, на понятийном и нормативном аппарате российского информационного права[31].

Понятием «компьютерная информация», используемым уголовным законодательством, охватывается и управляющая, и смысловая информация, закрепленная на цифровом носителе и (или) передаваемая по телекоммуникационным сетям[32].

Существует ряд иных сходных определений понятия «компьютерная информация», например, «электронная информация», которые, несомненно, представляют определенный научный интерес и научную ценность.

Так, А.В. Геллер, исследуя уголовно-правовые аспекты обеспечения защиты электронной информации, приходит к выводу, что электронная информация в рамках состава преступления представляет различные его (?) элементы (предмет и способ совершения преступления)[33].

По мнению В.Н. Щепетильникова, при формулировании объективной стороны преступлений гл. 28 «Преступления в сфере компью-

---

[29] Сивицкая Н. А. К вопросу об определении понятия «компьютерная информация» // Проблемы правовой информатизации. 2005. № 2. С. 35.

[30] Айсанов Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореф. дис. … канд. юрид. наук. М., 2006. С. 8.

[31] Гребеньков А. А. Общие подходы к определению понятия «компьютерная информация» в уголовно-правовой теории // Известия Юго-Западного государственного университета. Серия: История и право. 2012. № 1–2. С. 138.

[32] Кургузкина Е. Б., Ратникова Н. Д. Место совершения компьютерных преступлений // Вестник Воронежского института ФСИН России. 2016. № 1. С. 81.

[33] Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: автореф. дис. … канд. юрид. наук. М., 2006. С. 7.

терной информации» УК РФ целесообразно использовать выражение «электронная информация»[34]. Аналогичного мнения придерживаются Е.Г. Титарева[35] и М.А. Ефремова[36]. Мы в целом поддерживаем такую точку зрения, хотя далее предложим несколько развить ее.

Интересные предложения выдвигает П.Г. Смагин, который, основываясь на определении понятия «компьютерная информация», предложенном О.Г. Григорьевым[37], вводит свою дефиницию «электронная информация». Он пишет, что если информация была создана не на компьютере, а, к примеру, на цифровом фотоаппарате, то она уже не является компьютерной, но все равно зафиксирована в цифровом виде и при передаче ее на компьютер никакого искажения не произойдет. Он считает, что с появлением огромного количества цифровых устройств (сотовых телефонов, цифровых диктофонов, DVD-камер) понятие «компьютер» необходимо исключить из оборота в соответствующих законах, в том числе в УК РФ и иных нормативно-правовых актах, так как можно говорить только о цифровом устройстве[38]. Считаем, что с этой точкой зрения следует согласиться.

А.А. Нагорный под электронной информацией предлагает понимать сведения (сообщения, данные), представленные в цифровой форме и содержащиеся в информационно-телекоммуникационных

---

[34] Щепетильников В.Н. Уголовно-правовая охрана электронной информации: автореф. дис. … канд. юрид. наук. Елец, 2006. С. 7.

[35] См.: Титарева Е.Г. Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий // Научный альманах. 2015. № 7. С. 1160.

[36] См.: Ефремова М.А. Уголовно-правовая охрана информационной безопасности: автореф. дис. … д-ра юрид. наук. М., 2017. С. 20.

[37] См.: Григорьев О.В. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: автореф. дис. … канд. юрид. наук. Омск, 2007. С. 8.

[38] Смагин П.Г. О понятии «компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД // Вестник Воронежского института МВД России. 2008. № 1. С. 80.

устройствах, их системах и сетях. Он считает, что данное определение не лишено недостатков, однако оно способно наиболее полно отразить суть рассматриваемого явления[39].

Понятие «электронная» производно от греческого «электрон» – стабильная отрицательно заряженная элементарная частица, одна из основных структурных единиц вещества. Соответственно, электронная информация – информация, представленная в цифровой форме, не имеющая жесткой привязки к материальному носителю и преобразуемая для восприятия человеком в виде текста, изображения, звукового сигнала[40].

По мнению О. С. Герасимовой, не существует информации вообще, на каких бы носителях она ни закреплялась и с помощью каких бы технических средств она ни хранилась и ни передавалась. Это чисто теоретическое понятие. Практически существуют сведения конкретного содержания[41].

На наш взгляд, предметом преступления, посягающего на информацию в телекоммуникационных устройствах, их системах и сетях, следует признавать не компьютерную, а цифровую информацию. Под информацией в цифровой форме понимается информация в виде цифровой последовательности сигналов.

Следует отметить, что существует точка зрения, заключающаяся в необходимости использования в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ термина «электрон-

---

[39] Нагорный А. А. Содержания понятия компьютерной информации как предмета компьютерных преступлений // Актуальные проблемы российского права. 2014. № 8. С. 1697.

[40] Козаев Н. Ш. Современные информационные технологии как один из факторов развития уголовного права // Вестник Северо-Осетинского государственного университета им. К. Л. Хетагурова. 2013. № 3. С. 88.

[41] Герасимова О. С. Особенности преступлений в сфере компьютерной информации // Вестник ТГУ. 2007. № 12. С. 329.

но-цифровая информация», предложенного А. И. Маляровым[42]. Однако данное определение не совсем точно, так как цифровая информация является цифровой последовательностью по форме, но по виду изменяется в зависимости от среды распространения, т. е. от линии связи и канала передачи информации. Например, если цифровая информация передается в радиолинии связи, то она носит название электромагнитно-цифровой. Если по волоконно-оптической линии связи, то это оптико-цифровая информация. Очевидно, что электронно-цифровой информацией будет называться информация, передаваемая по проводным или кабельным линиям связи. Предложенный А. И. Маляровым к использованию термин «электронно-цифровая информация» не учитывает волоконно-оптические линии и радиолинии связи, в которых также циркулирует цифровая информация, и иные объекты.

Как отмечает В. В. Хилюта, любая компьютерная информация – это программа, которая состоит из набора символов «1» и «0»[43].

По нашему мнению, оригинальным и в то же время простым и точным представляется определение компьютерной информации, изложенное В. Б. Веховым, который предлагает под ней понимать сведения, находящиеся в памяти ЭВМ[44].

Кроме того, В. Б. Вехов указывает на основания классификации компьютерной информации как предмета совершения преступления:

– по юридическому положению (документированная и недокументированная);

---

[42] Маляров А. И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. … канд. юрид. наук. Краснодар, 2008. С. 9.

[43] Хилюта В. В. Правовая информатизация и уголовный закон // Проблемы правовой информатизации. 2007. № 1. С. 76.

[44] Вехов В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ // Уголовное право. 2004. № 4. С. 17.

– по категории доступности (общедоступная либо охраняемая законом – конфиденциальная информация или государственная тайна);

– по форме представления (электромагнитный сигнал, документальное сообщение, файл, программа для ЭВМ, база данных)[45].

Как отмечает И. А. Юрченко, особенностью информации является то, что ее невозможно представить без какой-либо материальной основы, она является атрибутом (свойством) материи и неотделима от нее. Даже тогда, когда информация отражается сознанием человека, она существует лишь в единстве с определенными нейрофизиологическими процессами, т. е. имеет свой материальный носитель[46].

Мы солидарны с мнением Н. А. Иванова, указывающего на общепризнанность общественностью понятия «цифровая информация». Он отмечает, что информация, вводимая, обрабатываемая и хранящаяся в устройствах памяти средств компьютерной и иной микропроцессорной техники или передаваемая по каким-либо каналам связи, имеет вид или зафиксирована (представлена) в виде дискретных сигналов, т. е. сигналов, имеющих конечное число значений. В средствах цифровой техники в подавляющем большинстве случаев используются сигналы только двух уровней. Поэтому информацию, представленную двумя уровнями дискретных сигналов, стали называть бинарной (двоичной). Наличие сигнала с определенными характеристиками стали считать за цифру «1», а сигнал другого уровня – за цифру «0». Соответственно информация, хранимая на машинных носителях, обрабатываемая средствами компьютерной или иной микропроцессорной техники и передаваемая по каким-либо линиям связи, получила

[45] Там же.

[46] Юрченко И. А. Информация конфиденциального характера как предмет уголовно-правовой охраны: автореф. дис. … канд. юрид. наук. М., 2000. С. 12.

название «цифровая информация». Данное определение стало общепризнанным, и под ней сегодня никто не подразумевает запись, исполненную цифрами арабской, римской или иной системы исчислений[47].

Рассмотрим толкование термина «цифровая информация» с трех позиций: филологической, технической и юридической[48].

Понятие «цифровая информация» является родовым по отношению к понятиям «компьютерная информация» и «электронная информация». Синонимия таких понятий, как «цифровая», «компьютерная» и «электронная» информация, ведет к неоправданному сужению признаков объективной стороны ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ.

В своем исследовании В. М. Гаврилов замечает, что термины «машинная информация», «компьютерная информация» и «электронная информация» не определены в законодательных и нормативных актах Российской Федерации. Они используются только для отражения специфической формы представления информации – в виде последовательностей (цепочек) двоичных кодов, с которыми работают только средства вычислительной техники. Эти последовательности двоичных кодов могут быть с помощью различных программ переведены в удобную для восприятия человеком форму: в читаемый текст, рисунок, звук, видео, закрепленную на немашинном (бумага, пленка, пластик, ткань и т. п.) носителе

[47] Иванов Н. А. О понятии «цифровые доказательства» и их месте в общей системе доказательств // Проблемы профилактики и противодействия компьютерным преступлениям: материалы Международной научно-практической конференции (г. Челябинск, 30 мая 2007 г.) и «круглого стола» (г. Челябинск, 18 мая 2007 г.) / отв. ред. А. В. Минбалеев. Челябинск: Челябинский центр по исследованию проблем противодействия организованной преступности и коррупции, 2008. С. 96.

[48] Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. … канд. юрид. наук. Казань, 2017. С. 29.

информации[49]. С первой половиной высказывания относительно определения в законодательных и нормативных актах Российской Федерации вышеназванных терминов следует согласиться, поскольку они действительно не нашли своего отражения ни в юридических источниках, ни в технических, т. к. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[50] и принятый вслед за ним национальный стандарт Российской Федерации ГОСТ Р 50922–2006 «Защита информации. Основные термины и определения»[51] относят всю совокупность информации к сведениям, независимо от формы их представления. Но мы не можем поддержать мнение о том, что последовательности двоичных кодов могут быть переведены в удобную для восприятия форму, так как цифровой код драйверов и других программ с легкостью можно распечатать и прочесть, но нельзя будет сделать с ним никаких манипуляций, как это сделали бы современные информационно-телекоммуникационные устройства.

Под цифровыми объектами понимаются информационно-программные продукты и другие результаты интеллектуальной деятельности, получаемые и используемые главным образом или исключительно в электронном (цифровом) виде. К ним относятся: электронные документы и издания, аудио-, видео-, мультимедийные продукты, программные средства, сайты, базы данных и дру-

---

[49] Гаврилов В. М. Противодействие преступлениям, совершаемым в сфере компьютерной и мобильной коммуникации организованными преступными группами. Саратов: Сателлит, 2009. С. 11.

[50] См.: Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 г. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

[51] См.: ГОСТ Р 50922-2006. «Защита информации. Основные термины и определения». М.: Стандартинформ, 2008. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 373-ст «Об утверждении национального стандарта». Текст приказа официально опубликован не был.

гие информационные массивы, промышленные образцы в виде компьютерной конструкторской документации, полезные модели в электронном виде, доменные имена и товарные знаки и др. Средой распространения цифровых объектов являются информационно-телекоммуникационные сети, и прежде всего сеть Интернет[52].

С точки зрения технического аспекта использование понятия «цифровая информация» как максимально широкой категории представляется наиболее удачным. Доказательством этому может служить следующий пример: человеческая речь во время телефонного сеанса связи является аналоговым сигналом. Далее речь преобразуется в последовательность двоичных символов в виде нулей и единиц[53]. Такая последовательность называется цифровой. На другом конце у абонента происходит обратный процесс, т.е. перевод цифровой информации в аналоговую информацию в форме звука.

Следует отметить, что по такому принципу работают все современные информационно-телекоммуникационные системы. Основным его преимуществом является легкость восстановления цифровой информации по сравнению с аналоговой при сбоях связи. Также цифровая информация менее подвержена искажению во время передачи. Кроме того, обмен данными в основном производится между двумя и более компьютерами, между компьютерами и цифровыми устройствами, а также между цифровыми устройствами в информационно-телекоммуникационной сети. Подобные цифровые устройства лучше обслуживаются цифровыми каналами связи[54].

---

[52] Антопольский А. Б. Государственный надзор и охрана прав владельцев цифровых объектов // Сборник тезисов докладов участников десятой Всероссийской конференции «Проблемы законодательства в сфере информатизации». М.: Изд-во «ВНИИПВТИ», 2002. С. 22.

[53] См.: Прокис Джон. Цифровая связь: пер. с англ.; под ред. Д. Д. Кловского. М.: Радио и связь, 2000. С. 7.

[54] Скляр Б. Цифровая связь. Теоретические основы и практическое применение: пер. с англ.; изд. 2-е, испр. М.: Издательский дом «Вильямс», 2003. С. 31.

Также представляется, что основным отличием цифровой информации от аналоговой является то, что первую можно без особых проблем копировать сколь угодно. При этом качество оригинала не изменится и не пострадает, что нельзя сказать относительно аналоговой информации. Так, при ксерокопировании обычного печатного листа в несколько приемов качество каждого последующего листа будет хуже предыдущего.

Что же касается компьютерной информации, то законодатель определил, что она циркулирует только в компьютерных системах, которые в свою очередь являются элементами современных информационно-телекоммуникационных систем. Таким образом, можно констатировать, что компьютерная информация является разновидностью цифровой информации.

Следует отметить, что С. П. Кушниренко также видит решение данной проблемы в пересмотре понятия предмета посягательства, названного в гл. 28 «Преступления в сфере компьютерной информации» УК РФ, и переходе к более общей его трактовке, а именно к понятию цифровой информации[55], хотя и этот термин на сегодняшний день еще однозначно не определен.

Определение понятия цифровой информации в уголовном праве и правильное раскрытие его содержания важны по нескольким обстоятельствам.

Прежде всего, для определения круга соответствующих преступных деяний и беспробельности правового регулирования. Так, посредством незаконного вмешательства в информационно-телекоммуникационные устройства, их системы и сети, в которых обращается цифровая информация, могут быть совершены преступления, предусмотренные ст. 105 «Убийство», 109 «Причинение смерти по неосторожности», 119 «Угроза убийством или причинением тяжкого

[55] Кушниренко С. П. Цифровая информация как самостоятельный объект криминалистического исследования // Вестник криминалистики. М.: Спарк, 2006. С. 43.

вреда здоровью», 137 «Нарушение неприкосновенности частной жизни», 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации», 146 «Нарушение авторских и смежных прав», 147 «Нарушение изобретательских и патентных прав», 155 «Разглашение тайны усыновления (удочерения)», 158 «Кража», 159 «Мошенничество», 159.1 «Мошенничество в сфере кредитования», 159.2 «Мошенничество при получении выплат», 159.3 «Мошенничество с использованием электронных средств платежа», 159.5 «Мошенничество в сфере страхования», 159.6 «Мошенничество в сфере компьютерной информации», 163 «Вымогательство», 165 «Причинение имущественного ущерба путем обмана или злоупотребления доверием», 171 «Незаконное предпринимательство», 174.1 «Легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления», 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», 187 «Неправомерный оборот средств платежей», 207 «Заведомо ложное сообщение об акте терроризма», 242 «Незаконные изготовление и оборот порнографических материалов или предметов», 242.1 «Изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних», 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование и распространение вредоносных компьютерных программ», 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», 275 «Государственная измена», 276 «Шпионаж», 282 «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства», 283 «Разглашение государственной тайны»,

284 «Утрата документов, содержащих государственную тайну», 303 «Фальсификация доказательств и результатов оперативно-разыскной деятельности», 306 «Заведомо ложный донос», 354 «Публичные призывы к развязыванию агрессивной войны» УК РФ.

С.П. Кушниренко предлагает понимать под цифровой информацией любую информацию, представленную в виде последовательности цифр, доступную для ввода, обработки, хранения, передачи с помощью технических устройств[56]. По нашему мнению, данное определение цифровой информации считать удачным в полной мере нельзя. Оно требует уточнения по следующим основаниям.

Во-первых, в нем ничего не говорится о технических средствах, предназначенных для ввода, обработки, хранения, передачи такой информации. Думается, что к таким средствам с технической точки зрения относятся разнообразные механические, электрические и другие устройства.

Во-вторых, нет необходимости указывать, в каком виде представлена цифровая информация, так как уже само название такой информации подразумевает ее цифровой вид.

В-третьих, словосочетание «доступную для ввода, обработки, хранения, передачи» представляется неточным, так как доступность ограничивает процесс обращения цифровой информации. Думается, что целесообразнее было бы заменить слово «доступную» на слово «предназначенную».

Сходные позиции отражены в трудах А.Г. Волеводза, который отмечает, что вся информация в компьютерах представляется в виде последовательностей нолей и единиц, т.е. работа компьютера основана на двоичной системе счисления[57].

Прежде чем предлагать свой вариант определения понятия «цифровая информация», необходимо выделить ее отличитель-

---

[56] Там же.

[57] Волеводз А. Г. Компьютерная информация как объект криминалистического следоведения. М.: Юрлитинформ, 2008. С. 341.

ные признаки и специфику. Проанализировав все вышеуказанные определения компьютерной и электронной информации, считаем необходимым отметить следующее.

Во-первых, цифровая информация проста в обрабатывании в информационно-телекоммуникационных устройствах независимо от их назначения, будь то персональный компьютер или сервер, мобильный телефон или планшетный компьютер, цифровая видеокамера или цифровой фотоаппарат.

Во-вторых, данная информация легко передается и обращается в информационно-телекоммуникационных устройствах, их системах и сетях.

В-третьих, эта информация легко создаваема и так же легко уничтожаема.

В-четвертых, данная информация может постоянно находиться лишь в информационно-телекоммуникационном устройстве или же временно в каналах и сетях передачи информации.

В-пятых, этот вид информации модифицируется и копируется без особых трудностей.

Из диспозиции ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ (в редакции до внесения в УК РФ изменений Федеральным законом от 7 декабря 2011 г. № 420-ФЗ[58]) следовало, что ответственность за неправомерный доступ к компьютерной информации наступает лишь в случае, если информация находится на машинном носителе, в ЭВМ, системе или сети ЭВМ. По логике законодателя получалось, что компьютерная информация – это информация, находящаяся исключительно на машинном носителе, в ЭВМ, системе или сети ЭВМ. Такое ограничение представляется не совсем верным, поскольку компьютерная информация могла находиться и в других устройствах, например мобильном телефоне.

[58] См.: О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 420-ФЗ от 7 декабря 2011 г. // СЗ РФ. 2011. № 50. Ст. 7362.

Более удачной видится формулировка, данная в ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ, в которой законодатель предпринял попытку учесть развитие информационно-телекоммуникационных технологий и расширить сферу обращения информации не только лишь машинным носителем и компьютером. Здесь законодатель вывел определение компьютерной информации из диспозиции ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ и дал ее определение в первом примечании к этой статье, согласно которому под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[59].

Используемая в УК РФ логика в части определения предмета преступления кардинально не изменилась. С точки зрения русского языка если информация обращается в компьютере, то она будет называться компьютерной, а следовательно, обращаемая информация в принтере будет называться принтерной, в сканере – сканерной и т. д. Широкое использование термина «компьютерная информация» представляется неточным и не соответствующим требованиям юридической техники[60].

С появлением современных беспроводных систем связи расширилась и сфера обращения информации. Поэтому в уточнении нуждается предмет преступления, предусмотренного ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ,– компьютерная информация, так как с технической точки зрения в современных информационно-телекоммуникационных системах

[59] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

[60] Бегишев И. Р. Правовые аспекты безопасности информационного общества // Информационное общество. 2011. № 4. С. 56.

обращается не компьютерная, а цифровая информация. Компьютерная информация является лишь подвидом цифровой информации.

Таким образом, предметом преступления, посягающего на информацию, обращающуюся в информационно-телекоммуникационных устройствах, их системах и сетях, следует признавать не компьютерную, а цифровую информацию.

В примечании 1 к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ предлагаем дать определение понятия «цифровая информация» вместо более узкого и менее точного понятия «компьютерная информация» в следующей авторской редакции:

> *«Под цифровой информацией понимаются сведения (сообщения, данные), обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях».*

Учитывая, что термин «цифровая информация» является более полным и точным, чем термин «компьютерная информация», рекомендуем использовать его в соответствующих статьях Особенной части УК РФ и отразить указанное понятие в ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В заключение параграфа следует отметить, что 92,86 % респондентов, принявших участие в экспертном опросе по проблемам уголовно-правового противодействия преступлениям в сфере обращения цифровой информации, считают, что термин «цифровая информация» является более широким по содержанию, чем термин «компьютерная информация»[61] (см. Приложения 1–3).

[61] Бегишев И. Р. Преступления в сфере обращения цифровой информации. Результаты научного исследования // Information Security / Информационная безопасность. 2012. № 6. С. 8.

§ 1.2. Понятие преступлений в сфере обращения цифровой информации

Теория и практика не выработали единого определения подобных преступлений. Эти правонарушения нередко именуются «компьютерными преступлениями». Однако представляется, что использовать термин «компьютерные преступления» в отношении данных деяний можно лишь с большой долей условности. Ведь к числу компьютерных можно относить как деяния, когда компьютер выступает в качестве предмета посягательства, так и деяния, в которых он является техническим средством совершения преступления. Эти случаи, а также использование компьютерной информации для совершения иных преступлений (например, мошенничества) не квалифицируются как преступления в сфере компьютерной информации (если нет совокупности преступлений). Например, посягательство на вычислительную технику: ее уничтожение, хищение – квалифицируется как преступление против собственности[62].

Необходимо согласиться с М. А. Ефремовой в том, что понятие компьютерных преступлений шире понятия преступлений в сфере компьютерной информации, они соотносятся как часть и целое[63].

Информационно-телекоммуникационные технологии, проникнув во все сферы жизни современного общества, являются их неотъемлемой составляющей и охватывают все ресурсы, обеспечивающие управление информацией, такие как компьютеры, телекоммуникационные сети, программное обеспечение[64].

---

[62] Компьютерные преступления // Словари и энциклопедии на Академике. URL: http://dic.academic.ru/dic.nsf/ruwiki/977065 (дата обращения: 23.05.2019).

[63] Ефремова М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий. М.: Юрлитинформ, 2015. С. 60.

[64] Хисамова З. И. Уголовная ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий. М.: Юрлитинформ, 2017. С. 8.

Темпы внедрения информационно-коммуникационных технологий в преступную деятельность настолько велики, что законодатель буквально не успевает за ними, ввиду чего становится актуальным вопрос об универсальности норм уголовного законодательства[65].

Несомненно, основными и наиболее наглядными для представления являются статистические данные о зарегистрированных преступлениях в сфере компьютерной информации, – данные, которые свидетельствуют о тревожных тенденциях.

Динамика зарегистрированных преступлений, совершенных в сфере компьютерной информации, с начала действия УК РФ показывала свой экспоненциальный рост вплоть до 2003 г. Так, в 1997 г. зарегистрировано 23 преступления, 1998 г.– 67, 1999 г.– 285, 2000 г.– 800, 2001 г.– 2 072, 2002 г.– 4 050. Это объясняется последствиями появления в уголовном законодательстве норм ответственности за преступления в сфере компьютерной информации, созданием подразделений правоохранительных органов, борющихся с преступлениями в сфере компьютерной информации, совершенствованием методик выявления и расследования указанных преступлений и становлением судебной практики по этим делам.

Несмотря на предпринятые законодателем меры, криминогенная ситуация в сфере обращения компьютерной информации за последние несколько лет коренным образом не изменилась. Об этом свидетельствуют данные статистической отчетности. Так, согласно сведениям ГИАЦ МВД России, в 2003 г. было зарегистрировано 7 540 преступлений, в 2004 г.– 8 739, 2005 г.– 10 214, 2006 г.– 8 889, 2007 г.– 7 236, 2008 г.– 9 010, 2009 г.– 11 636, 2010 г.– 7 398, 2011 г.– 2 698, 2012 г.– 2 820, 2013 г.– 2 563, 2014 г.– 1 739, 2015 г.– 2 382,

[65] Хисамова З. И. Уголовно-правовое противодействие новым видам угроз в информационной сфере // Вестник Краснодарского университета МВД России. 2015. № 4 (30). С. 136.

2016 г.– 1 748, 2017 г.– 1 883, а в 2018 г. было зарегистрировано 2 454 сообщения о преступлениях в сфере компьютерной информации[66].

Общие сведения о зарегистрированных в Российской Федерации преступлениях в сфере компьютерной информации за последние девять лет, а также сведения о зарегистрированных в указанный период преступлениях, предусмотренных гл. 28 «Преступления в сфере компьютерной информации» УК РФ, приведены в Приложениях 4, 6–8 настоящего исследования.

По нашему мнению, незначительное количество зарегистрированных преступлений в последние годы является подтверждением того, что в борьбе с преступлениями в сфере компьютерной информации правоохранительные органы, с одной стороны, сталкиваются с высочайшим уровнем латентности совершаемых преступниками деяний, недостаточной подготовкой специалистов для проведения компьютерно-технических экспертиз, а с другой – с несовершенством уголовно-правового законодательства.

Тем не менее очевидно, что, несмотря на высокую латентность указанных преступлений, их количество не превышает числа преступлений, связанных с незаконной игорной деятельностью, преступлений экстремистской направленности или связанных с оборотом порнографических материалов[67].

Заметим, что высокий уровень опасности рассматриваемых нами преступлений сохраняется также в связи с низкой эффективностью проведения дознания и предварительного следствия по этим делам, отсутствием в правоохранительных органах высококвалифицированных специалистов, расследующих преступления

---

[66] См.: Статистика и аналитика // Официальный сайт МВД России. – URL: https://mvd.ru/Deljatelnost/statistics (дата обращения: 23.05.2019).

[67] Петроченков С. Д. Криминологические особенности преступлений в сфере информационно-коммуникационных технологий // Вестник Московского университета МВД России. 2018. № 6. С. 158.

в сфере обращения цифровой информации, а также отсутствием единой уголовно-правовой политики в указанной сфере.

Возрастание числа пользователей информационно-телекоммуникационной сети Интернет не только способствует совершению в отношении них преступлений, но и расширяет возможности участия самих пользователей в преступной деятельности, в том числе в организованных формах. Отсутствие физических границ в сети Интернет позволяет совершать преступления как лицам, находящимся на территории Российской Федерации в отношении проживающих в других странах, так и лицам, находящимся за границей, в отношении потерпевших, пребывающих территориально в нашей стране[68].

Несмотря на весьма активное обсуждение этой проблемы, использование информационно-коммуникационных технологий в преступных целях в последние годы по-прежнему является серьезным вызовом как для правоохранительных, так и законодательных органов. Жертвами преступлений, совершаемых с использованием информационно-коммуникационных технологий, ежегодно становятся миллионы людей и организаций, а также органы власти конкретных государств[69].

Как отмечают в Управлении «К» МВД России, в преступном киберсообществе усиливаются специализация и разделение ролевых функций, улучшается координация и расширяется география

---

[68] Антонов О. Ю. Анализ преступной деятельности, совершаемой с использованием информационно-телекоммуникационных сетей // Вестник Академии Следственного комитета Российской Федерации. 2017. № 4 (14). С. 133.

[69] Русскевич Е. А. Проблемы систематизации современного уголовного законодательства об ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий (ИКТ) // Уголовная политика и правоприменительная практика: сб. ст. по мат. VI Международной науч.-практ. конф. Санкт-Петербург: Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия». СПб., 2019. С. 351–358.

деятельности злоумышленников. При этом сами преступления становятся все масштабнее и изощреннее, практически все они стали носить корыстный и межрегиональный характер, а их количество растет из года в год[70].

Необходимо отметить, что возрастает не только число зафиксированных инцидентов в рассматриваемой сфере, но и доходы лиц, виновных в их совершении.

По прогнозам ведущего мирового исследовательского центра по вопросам кибербезопасности *Cybersecurity Ventures*, мировой оборот киберпреступности достигнет $6 трлн в год к 2021 г. по сравнению с $3 трлн в 2015 г. Ожидается, что через три года киберпреступность будет более прибыльной, чем глобальная торговля всеми основными нелегальными наркотиками, вместе взятыми[71]. Возможно, это некоторое допущенное преувеличение, но оно говорит о темпах роста явления.

Как говорится в исследовании «Лаборатории Касперского», русскоязычные киберпреступники в период с 2012 по 2015 г. украли более 790 млн долларов. В зону их интересов входит весь мир. Эксперты уточняют: большую часть средств, а именно около 500 млн долларов, они получили за пределами постсоветского пространства. По оценке компании, в течение этих четырех лет в такой незаконной деятельности в России и сопредельных государствах участвовало около тысячи человек. Примерами крупных организованных преступных сообществ являются группировка *Carberp*, участники которой были арестованы в 2012–2013 гг., а также группировка *Carbanak*, раскрытая в начале 2015 г. Обе они выводили деньги

---

[70] Управление «К» выявило с начала года 7,5 тыс. преступлений в IT-сфере // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/news/24.11.2010/7020/ (дата обращения: 23.05.2019).

[71] Cybercrime Damages $6 Trillion By 2021 // Cybersecurity Ventures. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (дата обращения: 23.05.2019).

из банков путем заражения их *IT*-систем вредоносными компьютерными программами[72].

Однако существуют и иные статистические данные о количестве хакерских атак. Так, по данным авторитетной международной компании, специализирующейся в области информационной безопасности *Trustwave*, доля Российской Федерации в общемировом объеме компьютерных преступлений составляет 2,53 % и сопоставима с аналогичными показателями в Китайской Народной Республике[73].

В то же время интересными представляются данные, опубликованные компанией *Group-IB* (первой в России и в странах Содружества Независимых Государств компании, профессионально занявшейся расследованиями компьютерных инцидентов и преступлений), о доходах российских хакеров за свои услуги. Так, хищение номера кредитной карты оценивается от $5 до 25, гарантированный взлом почтового ящика – от $45, *DDOS*-атака на сайты – от $100, получение данных о банковских операциях жертвы – от $80 до 300, рассылка спама – $200, хищение номера кредитной карты с *PIN*-кодом – $500, создание вредоносных компьютерных программ для кражи информации – от $1 тыс. до 5 тыс.[74] Несомненно, что все эти цифры вызывают крайнюю озабоченность и указывают на огромные доходы такого криминального бизнеса.

В связи с высокой латентностью указанных преступлений статистические показатели не в полной мере отражают реальное положение дел в этой сфере.

---

[72] Коломыченко М. Киберпреступники сорвали банк // Коммерсантъ. 2015. № 213. С. 1.

[73] Чижов Д. Конец хакерской вольницы // Коммерсантъ Деньги. 2010. № 40. С. 42.

[74] Там же.

Для определения структуры преступлений в сфере компьютерной информации необходимо проанализировать судебную практику по указанной категории дел.

Так, основой исследования явился поиск упоминаний наименований ст. 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование и распространение вредоносных компьютерных программ», 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ в текстах материалов опубликованной судебной практики судов общей юрисдикции Российской Федерации, размещенных в открытом доступе на сайтах Государственной автоматизированной системы Российской Федерации «Правосудие» и справочно-правовой системы по судебным решениям «РосПравосудие» в период с 2010 по 2018 г. Всего в ходе исследования было изучено содержание более 250 обвинительных приговоров судов первой инстанции.

Наибольшая доля противоправных действий в рассматриваемой сфере приходится на неправомерный доступ к компьютерной информации (74 %) и на создание, использование и распространение вредоносных компьютерных программ (16 %). Также встречаются приговоры, в которых фигурирует незаконный оборот специальных технических средств, предназначенных для негласного получения информации (4 %) и мошенничества в сфере компьютерной информации (6 %), судебная практика по которым сложилась совсем недавно. Судебная практика по неправомерному воздействию на критическую информационную инфраструктуру Российской Федерации отсутствует.

Следует отметить, что в отечественной науке понятие «компьютерные преступления» тоже используется в широком и узком смыслах слова. В узком смысле – как синоним преступлений в сфере

компьютерной информации, а в широком – когда компьютер выступает орудием или средством совершения преступления, предметом преступления, характеризуют способ совершения преступления[75].

Так, М. А. Ефремова полагает, что компьютерная информация и устройства, на которых она зафиксирована или на которых она обращается, могут выступать средствами совершения преступлений. Из чего следует, что преступления, где компьютерная информация выступает средством совершения преступлений, образуют группу так называемых смежных преступлений и расположены в различных разделах и главах Особенной части УК РФ[76].

В данный момент существуют несколько точек зрения относительно понятия преступлений в сфере высоких технологий. Проблема точного определения этого понятия заключается в том, что практически невозможно выделить единый объект и предмет преступного посягательства, так как стремительное развитие информационно-телекоммуникационных технологий порождает новые объекты циркуляции цифровой информации.

З. И. Хисамова, проанализировав действующее законодательство и экономико-правовые реалии, пришла к выводу о том, что целесообразно использовать понятие «преступления, совершаемые в сфере использования информационно-коммуникационных технологий» для описания совокупности всех преступлений в сфере высоких технологий[77]. При этом под преступлениями, совершаемыми в сфере использования информационно-телекоммуникационных техноло-

---

[75] Лапунин М. М. Общая характеристика преступлений в сфере компьютерной информации // Право. Законодательство. Личность. 2013. № 1. С. 38.

[76] См.: Ефремова М. А. Уголовно-правовая охрана информационной безопасности. М.: Юрлитинформ, 2018. С. 226; Ефремова М. А. Уголовно-правовая охрана информационной безопасности: дис. … д-ра юрид. наук. М., 2017. С. 306.

[77] Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Юридическая наука и правоохранительная практика. 2015. № 3 (33). С. 127.

гий, З. И. Хисамова предлагает понимать виновные общественно опасные деяния, причиняющие ущерб общественным отношениям, связанным с безопасностью охраняемой законом информации, соблюдением установленного законом порядка оборота и использования информационно-телекоммуникационных технологий[78].

Соответственно выделяются два основных вида преступлений в сфере обращения цифровой информации: преступления, предметом которых является цифровая информация, и преступления, способом совершения которых являются цифровые технологии.

В настоящее время в уголовно-правовой науке сложилось три основных подхода к определению понятия преступления в сфере обращения цифровой информации.

Первая часть исследователей к компьютерным преступлениям относит деяния, в которых компьютер является объектом или орудием совершения преступления. Например, такой позиции придерживаются Н. И. Журавленко и Л. Е. Шведова[79], В. А. Номоконов и Т. Л. Тропина[80].

Вторая часть исследователей относит к компьютерным преступлениям только неправомерные действия в сфере обращения информации, циркулирующей в информационно-телекоммуникационных системах, в том числе неправомерный доступ к компьютерной информации.

Третья часть исследователей считает, что под компьютерными преступлениями следует понимать информационные преступле-

---

[78] См.: Хисамова З. И. Уголовная ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий. М.: Юрлитинформ, 2017. С. 40.

[79] См.: Журавленко Н. И., Шведова Л. Е. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой сфере // Общество и право. 2015. № 3. С. 67.

[80] См.: Номоконов В. А., Тропина Т. Л. Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2013. № 5. С. 150.

ния. Например, такой позиции придерживаются Л. А. Букалерова[81] и А. А. Шутова[82].

Последующая эволюция уголовного права определит жизнеспособность тех или иных терминов[83].

Существуют и противоположные точки зрения.

По мнению С. Ю. Бытко, появление компьютерной техники явилось просто следующим эволюционным этапом в истории хранения, передачи и обработки информации, значительно расширяющим возможности пользователей. Отличие компьютерной информации состоит лишь в форме ее представления, и, следовательно, компьютерная информация есть одна из возможных форм представления информации вообще[84]. Общественные отношения и интересы, ущерб которым может быть причинен незаконным собиранием, передачей или распространением соответствующих сведений, уже нашли свою уголовно-правовую охрану. Таким образом, помещение

---

[81] См.: Букалерова Л. А. Отсутствие главы в УК «Информационные преступления» – законодательный пробел // Пробелы в российском законодательстве. 2008. № 1. С. 256.

[82] См.: Шутова А. А. Информация как конструктивный признак отдельных составов преступлений // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 2 (30). С. 202; Шутова А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности. М.: Юрлитинформ, 2019. 192 с.; Шутова А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты: автореф. дис. … канд. юрид. наук. Н. Новгород, 2017. 22 с.; Шутова А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты: дис. … канд. юрид. наук. Н. Новгород, 2017. 264 с.

[83] См.: Арзамасцев М. В. К вопросу об уголовно-правовой классификации киберпреступлений // Актуальные вопросы права и отраслевых наук. 2017. № 1 (3). С. 11.

[84] Бытко С. Ю. Некоторые проблемы уголовной ответственности за преступления, совершенные с использованием компьютерных технологий: дис. … канд. юрид. наук. Саратов, 2002. С. 40.

преступлений в сфере компьютерной информации в УК РФ вносит в него избыточность[85].

Тождественной точки зрения придерживаются С. Ю. Трофимцева, Д. А. Илюшин и А. В. Линьков. Указанные ученые считают неправильным сохранение в УК РФ особой главы «Преступления в сфере компьютерной информации» и предлагают использовать опыт европейского законодателя, криминализировав ряд деяний в отношении компьютерной информации, систем и сетей ее обработки, хранения и передачи, и распределить составы компьютерных преступлений по другим главам УК РФ в зависимости от реального объекта каждого из преступлений такого вида[86]. С мнением названных авторов трудно согласиться, поскольку такое распределение нарушит структуру УК РФ, ведь рассматриваемые преступления действительно представляют собой самостоятельную группу родственных между собой деяний.

Также неоднозначно определено понятие сферы исследуемых преступных деяний, к которой некоторые исследователи относят информационные технологии, информационную безопасность, компьютерную и электронную информацию. Так, Д. В. Добровольский, раскрывая понятие преступлений в сфере информационных технологий, предлагает следующее определение: «Преступлениями в сфере информационных технологий являются предусмотренные уголовным законом виновные общественно опасные деяния, направленные на нарушение неприкосновенности охраняемой законом электронной информации и ее материальных носителей, совершаемые в процессе создания, использования и распространения электронной информации, а также направленные на нарушение работы ЭВМ, системы ЭВМ или их сети, причиняющие вред законным интересам

[85] Там же. С. 44.

[86] Трофимцева С. Ю., Илюшин Д. А., Линьков А. В. Объект компьютерных преступлений в российском и европейском уголовном праве: сравнительный анализ // Информационное противодействие угрозам терроризма. 2015. № 24. С. 9.

собственников или владельцев, жизни и здоровью личности, правам и свободам человека и гражданина, национальной безопасности»[87]. Т. Н. Богданова, соглашаясь с необходимостью внедрения в УК РФ термина «преступления в сфере информационных технологий», отмечает, что в таком случае объектом уголовно-правовой охраны будет выступать безопасность в этой сфере[88].

О. А. Савченко считает, что наименование главы 28 УК РФ в достаточной степени абстрактное. Понятие преступлений в сфере информационных технологий, напротив, является конкретным и исключающим разночтения в его толковании. Преступления в сфере информационно-телекоммуникационных технологий охватывают гораздо больший круг деяний, в их число входят любые преступления, совершенные в отношении и (или) с использованием информации, в том числе и компьютерной[89]. Аналогичную точку зрения высказывает и З. И. Хисамова[90].

В. А. Мазуров, исследуя преступность в сфере высоких технологий, делает вывод о том, что преступность в сфере высоких технологий – социально-правовое негативное явление, представляющее собой совокупность преступлений в сфере компьютерной информации[91].

---

[87] Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью: автореф. дис. … канд. юрид. наук. М., 2005. С. 8.

[88] Богданова Т. Н. К вопросу об определении понятия «преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. 2012. № 37. С. 66.

[89] Савченко О. А. Совершенствование уголовно-правового законодательства в сфере компьютерной информации на современном этапе развития информационных технологий // Законность и правопорядок в современном обществе. 2016. № 29. С. 156.

[90] Хисамова З. И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий // Юридический мир. 2016. № 2 С. 58–62.

[91] Мазуров В. А. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции // Вестник ТГУ. 2007. № 1. С. 154.

В свою очередь Т. Л. Тропина вводит новое понятие в вышеуказанной области – «киберпреступление»[92]. А. Н. Савиновский также рассматривает киберпреступность в качестве самостоятельного вида преступности[93].

Глобальное киберпространство и вся информационная среда в целом не материальны, поэтому их невозможно свести к физическому носителю, в котором они могут быть воплощены. Исходя из этого термин «компьютерная преступность» представляет собой несколько более узкое по своему смысловому значению понятие и сводит суть явления к преступлениям, которые совершаются с помощью компьютера[94].

Думается, не следует в определении понятия таких преступлений перечислять все противоправные деяния, направленные на завладение информацией.

Следует подчеркнуть, что перечень преступлений, совершаемых с использованием информационно-телекоммуникационных технологий, весьма значителен, и прогнозы по дальнейшей информатизации общества свидетельствуют о том, что он будет все более расширяться[95].

---

[92] Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 8.

[93] См.: Савиновский А. Н. Преступления в сфере компьютерной информации в законодательстве РФ // Экономика, социология и право. 2016. № 5. С. 115.

[94] Денисов Н. Л., Ромашкина Н. Ю. Анализ и оптимизация для единообразия правоприменения современного понимания киберпреступления // Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий: сборник материалов Межвуз. науч.-практ. конф. 19 апреля 2018 г. Рязань: Изд-во Рязанского филиала Московского университета МВД России имени В. Я. Кикотя, 2018. С. 122.

[95] Хисамова З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. … канд. юрид. наук. Краснодар, 2016. С. 46.

Общественно опасные деяния в области информационных правоотношений, представляющие угрозу общественной безопасности, особенно связанные с порядком применения компьютерной информации, получили наименование «преступления в сфере высоких технологий». К ним относят преступные деяния, совершенные с помощью вычислительной техники и средств телекоммуникаций, или такие, в которых объектом преступных посягательств выступает компьютерная информация[96].

М.В. Гаврилов также замечает, что, несмотря на широкое применение термина «компьютерные преступления» в литературе и средствах массовой информации, он не используется в законодательных и нормативных актах Российской Федерации. Это обстоятельство отражает тот факт, что общественно опасные действия, в которых либо средством, либо объектом преступного посягательства являются устройства вычислительной техники, но не изменяется «машинная» информация или не происходит раскрытие охраняемой законом «машинной» информации, не считаются «компьютерными преступлениями»[97].

На наш взгляд, следует согласиться с мнением В.М. Гаврилова, который считает, что в отличие от большинства других видов преступных деяний преступления в сфере компьютерной информации имеют свои специфические признаки:

– большая скрытность от человека и, как следствие, обнаружение факта совершения преступления со значительным опозданием, как правило, только после сверки бумажных документов и компьютерной информации;

– дистанционность – возможность значительного удаления местонахождения преступника и объекта преступления, не исклю-

[96] Пархомов В.А. К определению понятия «информационное преступление» // Вестник ИГЭА. 2001. № 2. С. 28.

[97] Гаврилов В.М. Противодействие преступлениям, совершаемым в сфере компьютерной и мобильной коммуникации организованными преступными группами. Саратов: Сателлит, 2009. С. 10.

чающая их расположение на территории разных государств, т.е. подпадание под юрисдикцию разных государств;

– сложность выявления и фиксации индивидуальной следовой информации, так как большинство «компьютерных преступлений» совершается с многопользовательских рабочих мест;

– сложность выявления и фиксации «компьютерной» следовой информации, учитывая возможность почти мгновенного изменения значительных по объему информационных массивов;

– сложность определения основных идентифицирующих характеристик преступления (даты, адреса, названия объектов и т.п.), учитывая простоту их замены преступником в случаях получения им полного контроля над компьютером-жертвой[98].

Учитывая все вышесказанное, мы предлагаем свое определение понятия преступления в сфере обращения цифровой информации, под которым предлагается понимать

> *предусмотренное уголовным законом виновное совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации.*

При этом защищаемыми свойствами цифровой информации ограниченного доступа являются ее конфиденциальность, целостность и достоверность, а общедоступной информации – ее целостность, достоверность и доступность.

Для правильной квалификации, точного применения и качественного расследования преступлений в сфере обращения цифровой информации необходимо классифицировать их по видам.

С учетом того, что спектр видов преступлений, направленных на завладение цифровой информацией, довольно разнообразен и постоянно изменяется, основным критерием, по которому можно

[98] Там же.

наиболее эффективно осуществить классификацию, является признаковый принцип, где предметом преступления будет выступать цифровая информация.

Предлагаем относить к преступлениям в сфере обращения цифровой информации деяния, предусмотренные ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации», 159.6 «Мошенничество в сфере компьютерной информации», 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование и распространение вредоносных компьютерных программ», 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ. Наиболее распространенными преступлениями являются преступления в сфере цифровой информации:

1) неправомерный доступ к цифровой информации;

2) создание, использование и распространение вредоносных компьютерных программ для информационно-телекоммуникационных устройств, их систем и сетей;

3) нарушение работы информационно-телекоммуникационных устройств, их систем и сетей;

4) неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Кроме того, довольно часто на практике встречаются случаи завладения информационно-телекоммуникационными устройствами обращения цифровой информации, перехвата цифровой информации, приобретения или сбыта цифровой информации, заведомо добытой преступным путем. Каждый из этих видов преступлений, направленных на завладение цифровой информацией, требует отдельной упорядоченной характеристики.

1. Неправомерный доступ к цифровой информации.

Неправомерный доступ – это доступ с нарушением установленных прав или правил. К этой группе преступлений необходимо относить все способы совершения преступления, которые приводят к нарушению конфиденциальности цифровой информации и связаны с обязательным наступлением следующих последствий: ознакомление, распространение, уничтожение, блокирование, модификация либо копирование цифровой информации. Также к таким преступным деяниям можно отнести задержки в передаче информации и искажения или нарушения целостности информации.

Например, Н. С. Мардер считает, что телекоммуникационная система может обеспечить абсолютную достоверную передачу информации, но время ее передачи может оказаться столь длительным, что она потеряет свою актуальность для потребителя. При искажении часть информации может быть утеряна, подменена другой информацией либо к исходной информации может быть добавлена информация, искажающая исходную[99].

2. Создание, использование и распространение вредоносных программ для информационно-телекоммуникационных устройств, их систем и сетей.

К таким способам совершения преступления относятся: способ непосредственного доступа к цифровой информации с последующей установкой вредоносной программы и способ опосредованного (удаленного) доступа к цифровой информации[100].

В качестве примера приведем приговор Октябрьского районного суда г. Кирова от 13 июля 2016 г. по уголовному делу № 1–298/2016. Суд установил, что для активации операционной системы *Windows* В. осуществил запуск с жесткого диска вредоносной компьютерной

[99] Мардер Н. С. Современные телекоммуникации. М.: ИРИАС, 2006. С. 197.

[100] См.: Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. М.: Щит-М, 1999. С. 110.

программы *RemoveWAT.exe*, тем самым умышленно использовал и распространил ее, что привело к нейтрализации системы защиты операционной системы *Windows*. Как следует из приведенного приговора, действия В. суд квалифицирует по ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ как распространение и использование компьютерной программы, заведомо предназначенной для блокирования компьютерной информации и нейтрализации средств ее защиты[101].

3. Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей.

К этой группе преступлений можно отнести действия, например, направленные на изменение нормального режима работы информационно-телекоммуникационных устройств, их систем и сетей.

Допустим, атака, которая стремится вызвать ложное срабатывание системы защиты информационно-телекоммуникационного устройства и таким образом привести к перегрузке системы, называется «отказ в обслуживании», или «*DoS*-атака»[102].

Атака в виде воздействия мощного электромагнитного импульса также может вывести из строя и нарушить работу информационно-телекоммуникационных устройств, их систем и сетей.

4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Национальное благополучие во многом сейчас зависит от безопасной и устойчивой критической инфраструктуры (системы и сети, лежащие в основе организации общества). Причинение критической информационной инфраструктуре ущерба может

---

[101] См.: Приговор Октябрьского районного суда г. Кирова от 13 июля 2016 г. по уголовному делу № 1–298/2016. URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-532913468/ (дата обращения: 23.05.2019).

[102] DoS-атака // Википедия: интернет-энциклопедия. URL: https://ru.wikipedia.org/wiki/DoS-атака (дата обращения: 23.05.2019).

привести к разрушающим и необратимым последствиям для их защищенности, а исходя из того, что КИИ выступает связующим звеном между другими областями национальной инфраструктуры, это неизбежно приведет к негативным для них последствиям[103].

5. Завладение информационно-телекоммуникационными устройствами обращения цифровой информации. К этой группе преступлений можно отнести действия, направленные на хищение чужого имущества, ответственность за которые предусмотрена ст. 158 «Кража», 160 «Присвоение или растрата», 161 «Грабеж», 162 «Разбой», 163 «Вымогательство» УК РФ. Имуществом здесь будут признаваться носители цифровой информации, к которым можно отнести жесткие диски, оптические диски, мобильные телефоны, планшетные компьютеры, персональные цифровые устройства, карты памяти, цифровые фотоаппараты и видеокамеры и т. д. Если осуществлено такое хищение либо вымогательство, а затем произведен неправомерный доступ к компьютерной информации, то содеянное следует дополнительно квалифицировать по ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ.

Довольно часто на практике имеет место утрата носителя цифровой информации, которая также может повлечь неправомерный доступ к компьютерной информации.

К. Е. Евдокимов предлагает дополнить гл. 28 «Преступления в сфере компьютерной информации» УК РФ следующей нормой: «Статья 272.1 «Незаконное завладение носителем компьютерной информации с целью осуществления неправомерного доступа к компьютерной информации»[104]. С учетом наших предложений

[103] Трунцевский Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 103.

[104] Евдокимов К. Н. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации // Вектор науки ТГУ. Серия: Юридические науки. 2014. № 4. С. 34.

о квалификации хищений и вымогательства информационно-телекоммуникационных устройств обращения цифровой информации и неправомерного доступа к компьютерной информации по совокупности считаем данное предложение хотя и вызванным объективными причинами, но уже учтенным уголовным законодательством.

6. Перехват цифровой информации.

В беспроводных системах обращения цифровой информации одним из основных общественно опасных способов завладения является перехват цифровой информации, так как в отличие от проводных систем передачи информации, которые могут быть атакованы только лишь из сети Интернет, беспроводные системы доступны для противоправных деяний со стороны злоумышленников ввиду специфики распространения информации в пространстве.

К современным беспроводным системам обращения цифровой информации можно отнести такие общепринятые системы, как *Bluetooth*, *Wi-Fi*, системы мобильной и спутниковой связи, а также другие информационно-телекоммуникационные системы, в которых цифровая информация передается посредством электромагнитного излучения в пространстве. Недостатком таких беспроводных систем является доступность передаваемой информации к перехвату с целью прочтения, копирования, разрушения и модификации.

Совершение перехвата цифровой информации в пространстве, наверное, невозможно без применения специальных технических средств, предназначенных для негласного получения информации, обращение которых запрещено.

Одним из видов перехвата информации является электромагнитный перехват, осуществляемый в помещениях, в которых находятся информационно-телекоммуникационные устройства. Он позволяет без прямого контакта с такими устройствами обращения цифровой информации перехватить возникающее при их функционировании электромагнитное излучение. Например, электронно-лучевая трубка монитора излучает в окружающее про-

странство электромагнитные волны, несущие в себе определенную информацию. Злоумышленники, перехватывая своей аппаратурой электромагнитные волны, передают их на компьютер, который отображает идентичное возникающему на мониторе «перехваченного» компьютера изображение[105].

7. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем.

Постоянные предложения приобрести различные базы персональных данных свидетельствуют о том, что продажа конфиденциальных сведений стала отдельным видом бизнеса. Способами такой добычи являются, прежде всего, хищения и вымогательство цифровой информации с целью последующего сбыта.

8. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

Этап проникновения в информационно-телекоммуникационные устройства с целью, например, копирования информации наступает только после этапа обхода или нарушения системы защиты цифровой информации, предусмотренной в таких устройствах, иначе заполучить цифровую информацию преступнику просто не удастся.

Современные информационно-телекоммуникационные устройства, системы и сети в основном хорошо защищены от атак на цифровую информацию, обращающуюся в них, так как находятся под охраной систем защиты цифровой информации.

К числу специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, можно отнести: сканеры портов информационно-телекоммуникационных устройств, программное обеспечение, предназначенное для дешифрования цифровой информации и для подбора паролей аутентификации, вредоносные компьютерные программы и т.д.

---

[105] Бегишев И. Р. Уголовная ответственность за перехват цифровой информации // Information Security / Информационная безопасность. 2010. № 4. С. 16.

К сожалению, в настоящий момент в информационно-телекоммуникационной сети Интернет находится огромный массив общедоступных программ, предназначенных для нарушения систем защиты цифровой информации, и каждый пользователь Сети может получить их совсем просто. Всеобщая распространенность таких специальных технических средств чревата трагическими последствиями[106].

Приведенная классификация показывает, что способы совершения преступлений в сфере обращения цифровой информации имеют свои индивидуальные черты. В большинстве своем все эти действия сопровождаются весьма квалифицированными способами маскировки, что само по себе затрудняет процесс выявления, раскрытия и расследования преступлений. Проведенное нами исследование показало, что очень часто преступниками используются различные количественные и качественные комбинации нескольких способов. По мере их модификации и постоянного усложнения логических связей появляются новые способы, отличительной особенностью которых является уже наличие сложных алгоритмов действий преступника, которые все более совершенствуются и модернизируются.

Кроме того, подавляющее большинство преступников, использующих вредоносные компьютерные программы, не являются их создателями, а приобретают их для преступных целей у представителей хакерского сообщества на специализированных сайтах, форумах или веб-страницах[107].

Необходимо отметить, что сеть Интернет содержит ресурсы, размещающие информацию о способах совершения преступлений

---

[106] Бегишев И. Р. Преступления в сфере цифровой информации: состояние, пробелы и пути их решения // Информационное право. 2010. № 2. С. 20.

[107] Евдокимов К. Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. 2016. № 2. С. 64.

в сфере компьютерной информации, а также объявления о предоставлении незаконных услуг в этой сфере. Думается, что законодателю необходимо ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации в сети Интернет и своевременно реагировать на ее появление[108].

Представляется, что ограничение доступа к такой информации возможно при условии дополнения п. 1 ч. 5 ст. 15.1 «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» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом:

> *«е) информации о способах совершения преступлений в сфере цифровой информации, а также объявлений по предоставлению незаконных услуг в этой сфере».*

§ 1.3. Феномен безопасной компьютерной атаки

Современные цифровые технологии существенно изменили процессы хранения, обработки и передачи цифровой информации. Процесс «цифровизации» общества охватывает все сферы деятельности государства и человека. Это во многом предопределило дальнейшее развитие информационных правоотношений и их правовое регулирование.

В связи с массовой информатизацией современного общества все большую актуальность приобретает знание способов

[108] Бегишев И. Р. Современное состояние преступлений в сфере обращения цифровой информации // Информация и безопасность. 2010. № 4. С. 569.

качественной защиты информационных технологий в повседневной практической деятельности. Наглядными примерами, иллюстрирующими необходимость защиты цифровой информации и обеспечения информационной безопасности, являются участившиеся сообщения о компьютерных взломах предприятий, росте компьютерного пиратства, распространении компьютерных вирусов[109].

Согласно данным аналитического центра компании «*InfoWatch*», в 2018 г. широко освещались утечки в *Acer*, *Amazon*, *Apple*, *Blizzard*, *Boeing*, *Facebook*, *HP*, *Huawei*, *Kmart*, *McDonald's*, *Microsoft*, *Netflix*, *PayPal*, *Samsung*, *Seagate*, *Sony*, *Telegram*, *Twitter*, *Valve*, *Yahoo*, ПриватБанке, министерствах иностранных дел Польши, Таиланда, Чехии, компрометация данных пользователей сервисов *Edmodo*, *Google Play*, *HipChat*, *Instagram*, *Snapchat*, *WhatsApp*[110].

Число компьютерных преступлений растет, увеличиваются масштабы компьютерных злоупотреблений. Умышленные атаки составляют заметную часть преступлений, но случайных действий пользователей, которые могут быть расценены как злоупотребления или ошибки, еще больше. И основной причиной потерь, как показывает практика, является недостаток информации о современных угрозах утечки конфиденциальных данных[111] и, как следствие, отсутствие адекватных мер противодействия таким угрозам.

---

[109] Современные угрозы, исходящие от информационных систем // Аналитический центр InfoWatch: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/docs/pamyatka_sovremenye_ugrozi_IW.pdf (дата обращения: 23.05.2019).

[110] Глобальное исследование утечек конфиденциальной информации в 2018 г. // Аналитический центр InfoWatch: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1 (дата обращения: 23.05.2019).

[111] Современные угрозы, исходящие от информационных систем // Аналитический центр InfoWatch: аналитический отчет. URL: https://www.infowatch.ru/sites/default/files/docs/pamyatka_sovremenye_ugrozi_IW.pdf (дата обращения: 23.05.2019).

Проблема противодействия преступлениям, совершаемым в сфере использования информационно-коммуникационных технологий, продолжает оставаться одной из наиболее злободневных[112].

Вместе с тем динамика развития информационно-телекоммуникационных технологий со всей очевидностью показывает, насколько значимой является проблема обеспечения безопасности информационной инфраструктуры[113], в том числе в деятельности субъектов информационных правоотношений.

К субъектам информационных правоотношений относят тех, кто наделен информационными правами и обязанностями, в том числе в части исполнения обязанностей по обеспечению безопасности информационной инфраструктуры.

Как правило, такая роль отводится руководителям и специалистам по информационной безопасности, защите информации, компьютерной безопасности, экономической безопасности, информационной безопасности телекоммуникационных систем, информационной безопасности автоматизированных систем управления, противодействию техническим разведкам и другим сотрудникам.

Однако воздействие на ход процессов защиты цифровой информации открывает новые возможности для совершенствования информационных правоотношений. Так, во время работы информационной инфраструктуры неизбежно могут возникать угрозы, связанные с совершением в отношении них компьютерных атак, т.е. попыток уничтожения, блокирования, копирования и модификации

---

[112] Хисамова З. И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. № 1 (55). С. 117.

[113] Под информационной инфраструктурой следует понимать совокупность информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления организаций.

цифровой информации, получения неправомерного доступа или иного несанкционированного вмешательства.

Общепринятый термин «компьютерная атака» (компьютерное вторжение, компьютерное нападение), разработанный специалистами государственного научно-исследовательского испытательного института проблем технической защиты информации Федеральной службы по техническому и экспортному контролю, а затем получивший широкое применение на практике, на наш взгляд, не дает точного определения происходящим неправомерным процессам. Утвержденный на основе предложений специалистов ФСТЭК России национальный стандарт Российской Федерации ГОСТ Р 51275–2006 раскрывает понятие «компьютерная атака» как целенаправленное несанкционированное воздействие на информацию, на ресурс информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных средств[114].

Кроме того, определение рассматриваемого понятия дается в федеральном законе, регулирующем отношения в области обеспечения безопасности критической информационной инфраструктуры при проведении в отношении ее компьютерных атак. В нем компьютерная атака определяется как целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования

[114] ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». М.: Стандартинформ, 2007. Утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии № 374-ст «Об утверждении национального стандарта» от 27.12.2006. Текст приказа официально опубликован не был.

и (или) создания угрозы безопасности обрабатываемой такими объектами информации[115].

В своем исследовании И. В. Котенко отмечает, что под атакой на компьютерную систему понимается любое воздействие злоумышленника на компьютерную систему с целью нарушения информационной безопасности, заключающееся в поиске и использовании той или иной уязвимости[116].

Близкую позицию занимает и А. Е. Боршевников, определяющий сетевую атаку как действие, целью которого является захват контроля (повышение прав) над удаленной/локальной вычислительной системой, либо ее дестабилизация, либо отказ в обслуживании, а также получение данных пользователей, пользующихся этой удаленной/локальной вычислительной системой[117].

По своей сути основными формами реализации атак и нарушения порядка функционирования информационно-телекоммуникационных систем могут быть:

– искажение информации;
– введение дезинформации;
– нарушение режимов функционирования;
– блокирование информации;
– разрушение информации;
– перехват информации;

---

[115] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // СЗ РФ. 2017. № 31 (часть I). Ст. 4736.

[116] Котенко И. В. Таксономии атак на компьютерные системы // Труды СПИИРАН. 2003. Т. 2, № 1. С. 196.

[117] Боршевников А. Е. Сетевые атаки. Виды. Способы борьбы // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). Уфа: Лето, 2011. С. 8.

– разглашение информации;

– хищение информации[118].

Мировой опыт реализации компьютерных атак показывает, что в 80 % случаев они совершаются собственными (иногда бывшими) сотрудниками организации или при их непосредственном участии. Именно такие внутренние нарушители информационной безопасности с полномочиями штатного пользователя или администратора системы представляют наибольшую опасность в современной российской действительности[119].

Таким образом, можно сделать вывод, что компьютерной атакой по смыслу рассматриваемых определений следует считать преднамеренные действия в отношении информационной инфраструктуры, повлекшие нарушение достоверности, целостности и конфиденциальности цифровой информации.

Что же касается собственно деятельности субъектов информационных правоотношений, то особенность их состояния в условиях непрерывного обеспечения защиты цифровой информации крайне важна как для практики применения информационного законодательства, так и для юридической науки, в частности, юридической психологии.

Г. Д. Бабушкин и В. И. Филиппенко к актуальным проблемам юридической психологии относят проблемы личности и деятельности в сфере реализации норм права, девиантного поведения и психологические аспекты его предотвращения[120].

При изучении видов цифровых преступлений, в частности, преступных посягательств на критическую информационную инфра-

---

[118] Малюк А. А. Организационно-методические проблемы обнаружения атак на объекты информационной инфраструктуры кредитно-финансовой сферы // Вопросы кибербезопасности. 2016. № 5. С. 9.

[119] Там же.

[120] Бабушкин Г. Д., Филиппенко В. И. Юридическая психология как научная дисциплина // Психопедагогика в правоохранительных органах. 1997. № 2. С. 116.

структуру[121], нами был обнаружен довольно интересный феномен (явление), связанный с деятельностью субъектов информационных правоотношений по вопросам обеспечения информационной безопасности своих информационных инфраструктур.

Практически каждый третий сотрудник знает, что сеть Интернет содержит огромное количество угроз (вредоносные компьютерные программы, мошенническое программное обеспечение и т. д.), но при этом не предпринимает усилий для защиты информационной инфраструктуры организации от угроз, надеясь на авось. Хотя приобретение и установка антивирусного программного обеспечения или превентивных средств защиты конфиденциальной информации (в том числе свободного распространения) оказали бы значительное влияние на уровень обеспечения информационной безопасности.

Соблюдение каждым сотрудником требований информационной безопасности носит индивидуальный характер и ставится в зависимость от его индивидуальных особенностей. Оно опосредовано таким качеством личности, как устойчивое субъективное отношение сотрудников к политике информационной безопасности

[121] Albrecht D. Chinese Cybersecurity Law Compared to EUNIS-Directive and German IT-Security Act. When cybersecurity not only protects interests of the masses but ultimately also safeguards national sovereignty // Recherchieren unter juris (Das Rechtsportal). 2018. Pp. 1–5; Bajramovic E. Cyber security in private industry critical infrastructure // International Journal of Economics and Law. 2015. № 13 (5). Pp. 9–15; Coman I. M. Cross-Border Cyber-Attacks and Critical Infrastructure Protection // International Journal of Information Security and Cybercrime. 2017. № 2 (6). Pp. 47–52; Venkatachary S. K., Prasad J., Samikannu R. Economic Impacts of Cyber Security in Energy Sector: A Review // International Journal of Energy Economics and Policy. 2017. № 7 (5). Pp. 250–262; The ITU publication Understanding cybercrime: phenomena, challenges and legal response has been prepared by Prof. Dr. Marco Gercke and is a new edition of a report previously entitled Understanding Cybercrime: A Guide for Developing Countries. The author wishes to thank the Infrastructure Enabling Environment and E-Application Department, ITU Telecommunication Development Bureau. URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx (дата обращения: 23.05.2019).

организации, к правилам защиты цифровой информации, к своим должностным обязанностям. Строгая дисциплина и культура информационной безопасности являются ключевым фактором в обеспечении цифровой безопасности.

Проведенный нами анализ более 150 приговоров, вынесенных федеральными судами общей юрисдикции по уголовным делам о преступлениях в сфере компьютерной информации (ст. 272 «Неправомерный доступ к компьютерной информации», 273 «Создание, использование и распространение вредоносных компьютерных программ», 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ[122]), и более 120 решений, вынесенных судебными участками мировых судей по делам об административных правонарушениях в области связи и информации (ст. 13.11 «Нарушение законодательства Российской Федерации в области персональных данных», 13.12 «Нарушение правил защиты информации», 13.13 «Незаконная деятельность в области защиты информации», 13.14 «Разглашение информации с ограниченным доступом» Кодекса Российской Федерации об административных правонарушениях[123]) за период с 2010 по 2018 г. и размещенных в открытом доступе на сайтах Государственной автоматизированной системы Российской Федерации «Правосудие» и справочно-правовой системы по судебным решениям «РосПравосудие» на территории 50 субъектов Российской Федерации, позволил сделать вывод о том, что поведение субъектов информационных правоотношений находилось во взаимосвязи с низкой психологической готовностью обеспечения информационной безопасности.

---

[122] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // СЗ РФ. 1996. № 25. Ст. 2954.

[123] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // СЗ РФ. 2002. № 1 (часть I). Ст. 1.

В ходе исследования определено, что для таких субъектов, помимо понимания механизмов обеспечения безопасности информационной инфраструктуры в условиях существования угроз их информационной безопасности, к сожалению, характерно снижение или полное игнорирование установленных требований по защите цифровой информации и политики информационной безопасности в силу различных причин.

К таким причинам рассматриваемого феномена можно отнести:

1) пренебрежение и халатность (некоторые сотрудники считают угрозы информационной безопасности информационной инфраструктуры надуманными, не соответствующими реалиям времени; некоторые собственники информационной инфраструктуры не заинтересованы в обеспечении их безопасности ввиду отсутствия позитивного экономического эффекта от этого);

2) нежелание нести значительные финансовые расходы на обеспечение информационной безопасности информационной инфраструктуры (высокая стоимость систем защиты цифровой информации, незаинтересованность в развитии систем информационной безопасности организации ввиду отсутствия финансовой выгоды и т.д.);

3) несоответствие систем защиты цифровой информации информационных систем и сетей уровню угроз их информационной безопасности (несоответствие средств защиты цифровой информации реальным и потенциальным угрозам информационной безопасности организации, отсутствие системы аудита информационной безопасности, увеличение количества атак на компьютерные системы и сети, сложность эксплуатации средств защиты цифровой информации и т.д.);

4) низкий уровень культуры информационной безопасности (низкая осведомленность руководителей и специалистов организаций об обеспечении информационной безопасности, игнорирование сотрудниками требований политики информационной безопасности организации, несоблюдение сотрудниками требований федерального законодательства в сфере защиты информации и т.д.);

5) нехватка квалифицированных специалистов по защите информации, в том числе специально-ориентированного профиля (специалистов по организации и реализации контроля защищенности, специалистов по оперативному мониторингу, обнаружению вторжений и сетевых атак, специалистов по обеспечению защиты от воздействия вредоносных программ и т. д.).

Кроме того, установлено, что потеря цифровой информации вследствие, например, неправомерного доступа к ней или действия вредоносной компьютерной программы во многом обусловлена отсутствием у сотрудников организаций знаний базовых основ обеспечения информационной безопасности[124].

В связи с изложенным выше предлагаем ввести в научный оборот термин «феномен безопасной компьютерной атаки» и определить его как состояние субъектов информационных правоотношений, осознающих опасность нарушения и важность обеспечения безопасности информационной инфраструктуры, но в силу различных причин не обеспечивающих ее, в том числе при проведении в отношении нее компьютерных атак. Безопасность атаки понимается в данном случае в ключе ее качества по отношению к атакующему.

Таким образом, среди основных личностных факторов, которые влияют на «феномен безопасной компьютерной атаки», следует выделить степень ответственности сотрудников за обеспечение информационной безопасности, выраженную в первую очередь в сохранении конфиденциальности цифровой информации и защите ее целостности и достоверности.

Думается, что данный термин может быть использован в качестве оценочного индикатора в системе обеспечения информационной безопасности субъектов информационных правоотношений.

---

[124] Бегишев И. Р. Синдром безопасной атаки: юридико-психологический феномен // Юридическая психология. 2018. № 2. С. 30.

Подводя итоги первой главы исследования, предлагаем следующие выводы:

1. Предметом преступления, посягающего на информацию, обращающуюся в информационно-телекоммуникационных устройствах, их системах и сетях, следует признавать не компьютерную, а цифровую информацию.

В примечании 1 к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ предлагаем дать определение понятия «цифровая информация» вместо более узкого и менее точного понятия «компьютерная информация» в следующей авторской редакции:

> *«Под цифровой информацией понимаются сведения (сообщения, данные), обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях».*

Учитывая, что термин «цифровая информация» является более полным и точным, чем термин «компьютерная информация», рекомендуем использовать его в соответствующих статьях Особенной части УК РФ и отразить указанное понятие в ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[125].

Следует отметить, что более 92 % респондентов, принявших участие в проведенном нами экспертном опросе по проблемам уголовно-правового противодействия преступлениям в сфере обращения цифровой информации, считают термин «цифровая

[125] Бегишев И. Р. Некоторые механизмы совершенствования уголовного законодательства за совершение преступлений в сфере обращения цифровой информации // Information Security / Информационная безопасность. 2017. № 6. С. 40.

информация» более широким по содержанию, чем термин «компьютерная информация»[126] (см. Приложения № 1–3).

2. В целях упорядочения терминологии, обеспечения единства и системности уголовного законодательства, основываясь на понятиях, используемых в федеральном законе, регулирующих отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации целесообразно использовать более широкий по содержанию термин «информационно-телекоммуникационные устройства, их системы и сети» в статьях Особенной части УК РФ вместо предусмотренного в ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ термина, указывающего на объекты обращения цифровой информации в виде «средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей».

3. *Под преступлением в сфере обращения цифровой информации предложено понимать предусмотренное уголовным законом виновное совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации.*

При этом защищаемыми свойствами цифровой информации ограниченного доступа являются ее конфиденциальность, целостность и достоверность, а общедоступной информации – ее целостность, достоверность и доступность.

---

[126] Бегишев И. Р. Преступления в сфере обращения цифровой информации. Результаты научного исследования // Information Security / Информационная безопасность. 2012. № 6. С. 8.

Следует отметить, что более 70 % респондентов, принявших участие в вышеуказанном социологическом опросе, считают приведенное определение верным[127].

4. Поскольку сеть Интернет содержит ресурсы, размещающие информацию о способах совершения преступлений в сфере компьютерной информации, а также объявления о предоставлении незаконных услуг в этой сфере, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «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» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом:

> *«е) информации о способах совершения преступлений в сфере цифровой информации, а также объявлений по предоставлению незаконных услуг в этой сфере».*

5. *Под компьютерной атакой* следует понимать преднамеренные действия в отношении информационной инфраструктуры, повлекшие нарушение достоверности, целостности и конфиденциальности цифровой информации.

6. Предложено ввести в правовую науку *термин «феномен безопасной компьютерной атаки» и определить его как состояние субъектов информационных правоотношений, осознающих опасность нарушения и важность обеспечения безопасности информационной инфраструктуры, но в силу различных причин*

[127] Там же.

не обеспечивающих ее, в том числе при проведении в отношении нее компьютерных атак.

Думается, что данный термин может быть использован в качестве оценочного индикатора в системе обеспечения информационной безопасности субъектов информационных правоотношений.

7. К таким *причинам феномена безопасной компьютерной атаки* можно отнести:

1) *пренебрежение и халатность* (некоторые сотрудники считают угрозы информационной безопасности информационной инфраструктуры надуманными, не соответствующими реалиям времени; некоторые собственники информационной инфраструктуры не заинтересованы в обеспечении их безопасности ввиду отсутствия позитивного экономического эффекта от этого);

2) *нежелание нести повышенные финансовые расходы на обеспечение информационной безопасности информационной инфраструктуры* (высокая стоимость систем защиты цифровой информации, незаинтересованность в развитии систем информационной безопасности организации ввиду отсутствия финансовой выгоды и т.д.);

3) *несоответствие систем защиты цифровой информации информационных систем и сетей уровню угроз их информационной безопасности* (несоответствие средств защиты цифровой информации реальным и потенциальным угрозам информационной безопасности организации, отсутствие системы аудита информационной безопасности, увеличение количества атак на компьютерные системы и сети, сложность эксплуатации средств защиты цифровой информации и т.д.);

4) *низкий уровень культуры информационной безопасности* (низкая осведомленность руководителей и специалистов организаций о вопросах обеспечения информационной безопасности, игнорирование сотрудниками требований политики информационной безопасности организации, несоблюдение сотрудниками

требований федерального законодательства в сфере защиты информации и т.д.);

5) *нехватка квалифицированных специалистов по защите информации, в том числе специально-ориентированного профиля* (специалистов по организации и реализации контроля защищенности, специалистов по оперативному мониторингу, обнаружению вторжений и сетевых атак, специалистов по обеспечению защиты от воздействия вредоносных программ и т.д.).

Кроме того, установлено, что потеря цифровой информации вследствие, например, неправомерного доступа к ней или действия вредоносной компьютерной программы во многом обусловлена отсутствием у сотрудников организаций знаний базовых основ обеспечения информационной безопасности.

ГЛАВА 2

ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО УГОЛОВНОМУ КОДЕКСУ РОССИЙСКОЙ ФЕДЕРАЦИИ КАК ВИДЫ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

§ 2.1. Неправомерный доступ к компьютерной информации

Существенным недостатком действующего российского уголовного закона является несоответствие терминологии ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ современному состоянию науки и техники, которое вызвано целым рядом причин. Справедливым в этой связи видится мнение Н. Ф. Кузнецовой о том, что в уголовном праве юридическая междисциплинарность и метасистемность, т. е. взаимодействие с другими отраслями науки, разработаны недостаточно[128]. Считаем обеспечение гармонизации терминологии УК РФ и положений различных наук важным направлением совершенствования российского уголовного закона.

[128] Кузнецова Н. Ф. Историко-сравнительный анализ уголовно-правовых отраслей науки, законодательства и правоприменения // Российский криминологический взгляд. 2008. № 1. С. 130.

Сосредоточимся на нескольких наиболее важных, на наш взгляд, проблемах такого несоответствия.

1. В ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ установлена ответственность за неправомерный доступ только к охраняемой законом компьютерной информации, хотя помимо компьютерных систем такая же по структуре информация находится и в телекоммуникационных системах, в числе которых системы электросвязи, радиосвязи и радиовещания, радиорелейной и спутниковой связи, системы мобильной связи, системы беспроводного доступа. Хотя теперь примечание 1 к ст. 272 определяет компьютерную информацию как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, все равно применительно к данной норме сам термин использовать представляется неудачным, поскольку он вводит в заблуждение, фактически делая отсылку к компьютерам.

А. И. Маляров в целом верно определяет направления совершенствования ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, предлагая указать, что информация находится также в информационных системах или информационно-телекоммуникационных системах[129], однако предложенные им термины обладают определенной неточностью. Например, за рамками названных систем или сетей находятся такие объекты, как собственно телекоммуникационные устройства, в числе которых абонентские станции мобильной связи, аппаратура коммутации связи и другие устройства, а также системы и сети проводной, оптической и радиосвязи.

2. В ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ законодатель ранее, до декабря 2011 г., называл

[129] Маляров А. И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. … канд. юрид. наук. Краснодар, 2008. С. 9.

одним из объектов нахождения информации машинный носитель. Думается, что к машинным носителям могут относиться носители информации в виде машин, механизмов и различных агрегатов. Когда законодатель вводил термин «машинный носитель», то он, по-видимому, подразумевал под ним элемент хранения информации, являющийся частью компьютера. Однако телекоммуникационные системы по сути своей не являются машинами. Современными носителями цифровой информации, кроме компьютеров, являются различные флеш-накопители, съемные жесткие диски, компакт-диски и т. д., которые, на наш взгляд, не подпадают под категорию машинных носителей, поскольку не являются частью той или иной машины.

В связи с изложенным мы поддерживаем решение законодателя об исключении термина «машинный носитель» из диспозиции ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ.

Используя устоявшуюся у специалистов формулировку, предлагается ввести обобщенное понятие устройств, систем и сетей, в которых обращается цифровая информация, и определить их по совокупности как информационно-телекоммуникационные устройства, системы и их сети.

На наш взгляд, в действующем уголовном законодательстве Российской Федерации недостаточно уделено внимания уголовно-правовой ответственности за перехват цифровой информации, который, как мы считаем, требует более внимательного изучения[130].

Отмечается, что в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ необходимо предусмотреть дополнительные квалифицирующие признаки, которые бы предусматривали

[130] Бегишев И. Р. Перехват охраняемой законом цифровой информации: уголовно-правовые аспекты // Информационная безопасность регионов. 2011. № 1. С. 79.

дифференциацию способа получения доступа к компьютерной информации[131].

Следует отметить, что наряду со стремительным развитием беспроводных систем обращения цифровой информации увеличилось производство и распространение специальных технических средств, предназначенных для негласного получения информации, в том числе для радиомониторинга и радиоперехвата. При этом вероятность поимки злоумышленников ничтожно мала ввиду отсутствия материальных следов совершения преступления.

Принято считать, что основным способом совершения противоправного деяния в сфере компьютерной информации является неправомерный доступ к компьютерной информации.

Понятие «неправомерный доступ», используемое в диспозиции ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, не исчерпывает весь круг способов посягательств на информацию, находящуюся на объектах обращения информации. Кроме того, в связи с увеличением сферы обращения цифровой информации появляются и новые способы совершения деяний, посягающих на цифровую информацию, циркулирующую, например, в сетях мобильной, спутниковой связи и беспроводного доступа. Основным видом преступного посягательства на цифровую информацию в таких информационно-телекоммуникационных системах является перехват цифровой информации, совершенный с помощью специальных технических средств. При этом цифровая информация преобразуется в электромагнитные излучения для передачи в пространстве, что является основой всех беспроводных систем передачи данных.

---

131 Денисов Н. Л. Несоответствие современным реалиям существующей уголовной ответственности за неправомерный доступ к компьютерной информации // Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий: сборник материалов Межвуз. науч.-практ. конф., 19 апреля 2018 г. Рязань: Изд-во Рязанского филиала Московского университета МВД России имени В. Я. Кикотя, 2018. С. 106.

Посягательства на цифровую информацию могут выражаться также в использовании информационно-телекоммуникационных технологий с целью пропаганды идеологии терроризма, ксенофобии, экстремизма, распространения идей национальной исключительности, дестабилизации общественно-политической обстановки в стране и т. п.[132]

Под неправомерным доступом Ф. С. Воройский понимает доступ к информационным или вычислительным ресурсам системы лиц, не имеющих права пользования ими[133]. Доступ можно рассматривать и как состояние (последствие действий), и как процесс (сами действия). Доступ будет являться неправомерным, если лицо не имеет права доступа к компьютерной информации. Уголовной ответственности лицо должно подлежать как в случае неправомерного доступа-состояния, так и в случае неправомерного доступа-процесса[134].

Основное отличие перехвата от несанкционированного доступа, по нашему мнению, заключается в том, что электромагнитному перехвату подвержена цифровая информация, циркулирующая в пространстве, а неправомерный доступ требует нарушения системы защиты информации информационно-телекоммуникационного устройства[135].

Предметом данного преступления может выступать охраняемая законом цифровая информация о государственной тайне, коммерческой тайне и т. д.

---

[132] Нечаева Е. В. Посягательства на цифровую информацию: современное состояние проблемы // Человек: преступление и наказание. 2019. Т. 27 (1–4). № 1. С. 81.

[133] Воройский Ф. С. Информатика. Энциклопедический словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах. М.: Физматлит, 2006. С. 365.

[134] Ефремова М. А. Ответственность за неправомерный доступ к компьютерной информации по действующему уголовному законодательству // Вестник Казанского юридического института МВД России. 2012. № 8. С. 56.

[135] Бегишев И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: авто-реф. дис. … канд. юрид. наук. Казань, 2017. С. 20.

Как известно, существует множество вредоносных компьютерных программ, специально разработанных для взлома беспроводных систем и доступных в сети Интернет. Работа таких программ основана на перехвате сетевых пакетов, их анализе для получения пароля доступа с последующим раскодированием перехваченных файлов.

В беспроводных системах обращения цифровой информации одним из основных общественно опасных способов завладения цифровой информацией является перехват информации, так как в отличие от проводных систем передачи информации, которые могут быть атакованы лишь из сети Интернет, беспроводные системы доступны для противоправных деяний со стороны злоумышленников ввиду специфики распространения информации в пространстве.

Следует отметить, что в системах спутниковой, мобильной и иной беспроводной связи, в которых объектом преступных посягательств выступает цифровая информация, информация передается посредством электромагнитных сигналов, причем независимо от природы ее передачи. Так, в качестве электромагнитных сигналов для передачи по беспроводным каналам связи в основном используются радиосигналы.

По способу совершения перехват цифровой информации в пространстве невозможен без применения специальных технических средств, предназначенных для негласного получения информации, обращение которых ограничено.

Огромным преимуществом добывания информации с помощью перехвата для злоумышленника представляется то, что такое деяние не оставляет за собой следов и потому является исключительно высоколатентным.

Для совершения перехвата цифровой информации, излучаемой в пространстве, злоумышленники обычно совершают следующие действия:

– сканирование атакуемой сети беспроводной связи на предмет поиска излучаемого в пространстве необходимого электромагнитного сигнала (цифровой информации);

– перехват цифровой информации в пространстве и ее запись;

– дешифрование (с помощью специального программного обеспечения) перехваченной цифровой информации с последующим ее представлением в форме, доступной для понимания.

Одним из видов перехвата информации является электромагнитный перехват, осуществляемый в помещениях, в которых находятся информационно-телекоммуникационные устройства. Он позволяет без прямого контакта с такими устройствами обращения цифровой информации перехватить электромагнитное излучение, возникающее при функционировании таких устройств. Например, экран монитора излучает в окружающее пространство электромагнитные волны, несущие в себе определенную информацию. Злоумышленники, перехватывая своей аппаратурой электромагнитные волны, передают их на компьютер, который воссоздает изображение, идентичное возникающему на мониторе «перехваченного» компьютера.

Следует отметить, что перехват цифровой информации возможен и в процессе радиоконтроля за излучениями радиоэлектронных средств. В соответствии со ст. 25 «Контроль за излучениями радиоэлектронных средств и (или) высокочастотных устройств» Федерального закона «О связи»[136] в процессе радиоконтроля для изучения параметров излучений радиоэлектронных средств и (или) высокочастотных устройств, а также для подтверждения нарушения установленных правил использования радиочастотного спектра может проводиться запись сигналов контролируемых источников излучений. Такая запись может служить лишь доказательством нарушения порядка использования радиочастотного спектра. Использование этой записи в иных целях не допускается, и виновные в таком использовании лица несут установленную законодатель-

[136] О связи: Федеральный закон № 126-ФЗ от 07 июля 2003 г. // СЗ РФ. 2003. № 28. Ст. 2895.

ством Российской Федерации ответственность за нарушение неприкосновенности частной жизни, личной, семейной, врачебной, коммерческой и иной охраняемой законом тайны.

Перехват информации возможен и в самой распространенной системе беспроводной связи – мобильной. Так, на хакерской конференции *Chaos Communication Congress* был представлен проект, позволяющий осуществить прослушивание любого мобильного телефона. Эксперты по информационной безопасности систем мобильной связи опубликовали инструкции по взлому алгоритма шифрования мобильной связи и создания устройства, способного перехватить трафик с мобильного телефона. Криптографам удалось взломать секретный код, который используется для предотвращения перехвата радиосигналов между конечным устройством и базовой станцией оператора. Код используется для предотвращения перехвата звонков путем частой смены радиочастот в спектре 80 каналов. Без знания точной последовательности переключений возможно перехватить только некоторые отрывки разговора[137].

Таким образом, общественная опасность неправомерного доступа к цифровой информации соизмерима с опасностью деяния, совершенного путем перехвата цифровой информации в пространстве. Учитывая, что ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ не включает в себя указание на такое противоправное действие, как перехват цифровой информации, и в связи с вышесказанными пробелами предлагается установить ответственность за перехват охраняемой законом цифровой информации и внести соответствующие изменения в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ.

---

[137] См.: Найдена уязвимость в алгоритме, позволяющая прослушивать мобильные телефоны // Информационный портал по безопасности SecurityLab.ru. URL: http://www.securitylab.ru/news/389223.php?pagen=2&el_id=389223 (дата обращения: 23.05.2019).

В примечании 3 к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ предлагаем дать определение понятия «перехват цифровой информации» в следующей редакции:

«Под перехватом цифровой информации понимается процесс неправомерного ее получения в пространстве».

Что касается вопросов криминализации незаконного ознакомления с охраняемой законом цифровой информацией, то среди исследователей данной проблемы имеются различные мнения.

Обязательным признаком объективной стороны преступления, предусмотренного ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, являются последствия в виде уничтожения, блокирования, модификации либо копирования информации.

Это означает, что, несмотря на то, что доступ к компьютерной информации может быть неправомерным, если он не повлек за собой перечисленных в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ последствий, он не может считаться преступлением.

Таким образом, не наказуемо в уголовно-правовом порядке деяние, в результате которого указанные в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ последствия не наступают, а цифровая информация становится известна третьему лицу в процессе, например, чтения информации с экрана компьютера. Между тем такое деяние способно причинить имущественный ущерб или иной вред ее обладателю.

Следует отметить, что в перечень деяний, повлекших за собой неправомерный доступ, не входит такое деяние, как ознакомление.

Предложения о введении дополнительного последствия в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в виде ознакомления с информацией исследовались двумя учеными: В. Н. Щепетильниковым и С. А. Яшковым. В. Н. Щепетильников справедливо указал, что незаконный доступ к компьютерной ин-

формации включает в себя ознакомление с ней[138]. В свою очередь, С. А. Яшков считает необходимым включить в УК РФ деяние, повлекшее полное либо частичное ознакомление с компьютерной информацией[139].

На наш взгляд, ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ не регулирует ситуацию, при которой вследствие неправомерного доступа к цифровой информации происходит ознакомление с ней, что исключает ответственность за огромный пласт возможных преступных посягательств. Между тем виновный может просто прочитать хранящуюся в памяти компьютера информацию, а затем использовать полученные знания в своих целях. Указанное деяние также заслуживает, на наш взгляд, уголовной ответственности.

Поддерживая позицию С. А. Яшкова и учитывая, что ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ не содержит указания на такой способ преступления, как ознакомление с цифровой информацией, предлагаем дополнить данную норму словом «ознакомление».

Существенным недостатком ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ является несоответствие ее терминологического аппарата современному состоянию научно-технического прогресса. В связи с этим встает вопрос о решении данного пробела путем совершенствования и модернизации соответствующей нормы.

Для этого следует обратиться к основному закону, регулирующему отношения в сфере информации. Ст. 15 «Использование информационно-телекоммуникационных сетей» Федерального

---

[138] Щепетильников В. Н. Уголовно-правовая охрана электронной информации: автореф. дис. … канд. юрид. наук. Елец, 2006. С. 6.

[139] Яшков С. А. Информация как объект преступления: автореф. дис. … канд. юрид. наук. Екатеринбург, 2005. С. 8.

закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[140] говорит об использовании информационно-телекоммуникационных сетей на территории Российской Федерации.

Думается, что данное словосочетание больше всего подходит для определения сферы обращения цифровой информации, так как оно реально соответствует современному состоянию обращения цифровой информации, в его содержание входят и компьютерные сети, и иные сети связи.

Н. Н. Куняев предлагает использовать в нормах права более широкое понятие – «информационно-коммуникационные технологии», которое, по его мнению, является базовым применительно к информационной сфере. Он считает, что «информационно-коммуникационные технологии» – это средства, способы, методы, механизмы, применяемые для создания, сбора, фиксации, передачи, распространения, блокировки, обработки, копирования, модификации, использования, защиты, хранения и уничтожения информации[141]. Мы поддерживаем данную позицию, соответствующую современному уровню развития информационных технологий.

В условиях формирования глобального информационного общества огромное значение придается проблеме обеспечения безопасности информации, в частности, вопросам противодействия преступным посягательствам в сфере ее обращения. Всеобщая информатизация общества обострила указанную проблему, возникла насущная потребность разработки и проведения соответствующей государственной политики. В последние пятнадцать лет в Россий-

[140] О связи: Федеральный закон № 126-ФЗ от 7 июля 2003 г. // СЗ РФ. 2003. № 28. Ст. 2895.

[141] Куняев Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: автореф. дис. … д-ра юрид. наук. М., 2010. С. 12.

ской Федерации появились и успешно освоены новые виды систем обращения информации, в числе которых системы мобильной, спутниковой, цифровой проводной, а также различные системы персональной беспроводной связи. Это свидетельствует о необходимости постоянного учета в тексте уголовного закона самых последних достижений науки и техники: нормативное регулирование не должно отставать от жизненных реалий.

Основным фактором повышенного внимания со стороны злоумышленников к циркулирующей в рассматриваемых системах информации является ее конфиденциальность. Преступники пытаются завладеть информацией, которая представляет для них ценность, не имея на то законного права.

Традиционно принято считать, что самыми распространенными преступлениями, предусмотренными гл. 28 «Преступления в сфере компьютерной информации» УК РФ, являются преступления, ответственность за которые наступает по ст. 272 «Неправомерный доступ к компьютерной информации» и ст. 273 «Создание, использование и распространение вредоносных компьютерных программ». Если в 2017 г. зарегистрировано 1 883 таких преступления (+7,7 %), то за первое полугодие 2018 г.– 1 233 (+3,4 %)[142].

Хотя законодатель предпринял попытку улучшить ситуацию с компьютерной преступностью в России, приняв Федеральный закон от 07 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации»[143], подробный анализ содержания ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в новой редакции показывает наличие как минимум нескольких непростых вопросов, без решения которых трудно говорить об

[142] Генпрокуратура: число преступлений в IT-сфере возросло // РосКомСвобода. URL: https://roskomsvoboda.org/40924 (дата обращения: 23.05.2019).

[143] См.: СЗ РФ. 2011. № 50. Ст. 7362.

эффективной уголовной политике в этой рассматриваемой сфере и которые далее мы постараемся разобрать и проанализировать[144].

Из анализа ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ вытекает, что преступление считается оконченным, когда незаконный доступ к компьютерной информации повлек за собой уничтожение, блокирование, модификацию либо копирование компьютерной информации.

По сравнению с прежней редакцией статьи исключены такие обязательные и альтернативные одновременно последствия преступления, как нарушение работы ЭВМ, системы ЭВМ или их сети, что представляется нам спорным. Результаты неправомерного доступа не только могут вызвать, например, временные сбои в работе всей информационной системы организации, но и парализовать ее на длительное время. Наступление подобных последствий свидетельствует об общественной опасности деяния, которое, на наш взгляд, заслуживает уголовной ответственности. Поэтому в число альтернативных последствий, предусмотренных ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, следует включить «нарушение работы информационно-телекоммуникационных устройств, их систем и сетей». Указанные предметы имеют более обобщенное и точное содержание, чем старые «ЭВМ, системы ЭВМ или их сети».

В ч. 2 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в редакции Федерального закона 7 декабря 2011 г. № 420-ФЗ от появились такие новые квалифицирующие признаки, как причинение деянием крупного ущерба или совершение его из корыстной заинтересованности. Причем законодатель определил,

[144] Бегишев И. Р. Новое в ответственности за неправомерный доступ к компьютерной информации по Уголовному кодексу Российской Федерации // Правосудие в Татарстане. 2011. № 4. С. 42.

что крупным признается ущерб, сумма которого превышает один миллион рублей. Видится, что, вводя такие признаки, законодатель идет по пути дифференциации уголовной ответственности. Вместе с тем установление такого значительного размера ответственности является неоправданным. Ущерб в несколько десятков или сотен тысяч рублей для граждан или субъектов малого бизнеса вполне может иметь фатальные последствия. Размер в сто тысяч, на наш взгляд, тоже заслуживает отнесения к крупному. Либо, возможно, указанный признак следовало бы сделать оценочным.

Кроме того, предлагаем использовать дополнительные квалифицирующие признаки, такие как совершение деяния из хулиганских побуждений, с использованием специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. Такие признаки представляются нам верными и соответствующими реальной действительности.

В ч. 4 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ установлена ответственность за деяния, предусмотренные предыдущими частями этой статьи, если они повлекли тяжкие последствия или создали угрозу их наступления. Хотелось бы, чтобы законодатель в примечании к статье перечислил хотя бы примерный перечень таких последствий, что, безусловно, облегчило бы работу правоприменителя. Безусловно, сюда должны относиться такие последствия, как причинение смерти либо тяжкого вреда здоровью по неосторожности.

Видится правильным решение законодателя о предусмотрении в законе названных особо квалифицирующих признаков.

Поиск упоминания наименования ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ в текстах материалов опубликованной судебной практики судов общей юрисдикции Российской Федерации, размещенных в открытом доступе на сайтах Государственной автоматизированной системы Российской Федерации «Правосудие» и справочно-правовой системы по судебным

решениям «РосПравосудие», позволил проанализировать судебную практику по указанной категории дел и показать структуру данного преступления[145].

Среди преступлений, предусмотренных ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, наибольшую часть (85 %) составляют преступления, выраженные в краже логинов и паролей для получения бесплатных услуг по доступу к сети Интернет, к почтовым ящикам пользователей, а также иного финансового обогащения. Оставшиеся 15 % приходятся на иные виды неправомерного доступа к компьютерной информации.

Так, Трусовским районным судом г. Астрахани вынесен приговор по обвинению гр. Ш. в совершении преступления, предусмотренного ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ. Суд установил, что гр. Ш. совершал незаконный доступ к компьютерной информации с целью получения бесплатных услуг по доступу к сети Интернет. Так, гр. Ш. через сервер провайдера путем вышеуказанных подключений и внесения учетных записей посредством пароля и логина, принадлежащих гр. М., неправомерно подключился к серверу провайдера для

---

[145] См., например: Приговор Надымского городского суда Ямало-Ненецкого автономного округа от 18 августа 2010 г. по уголовному делу № 1-248/2010. URL: https://rospravosudie.com/court-nadymskij-gorodskoj-sud-yamalo-neneckij-avtonomnyj-okrug-s/act-104979780 (дата обращения: 23.05.2019); Приговор Промышленного районного суда г. Оренбурга от 21 февраля 2011 г. по уголовному делу № 1-55/2011. URL: https://rospravosudie.com/court-promyshlennyj-rajonnyj-sud-g-orenburga-orenburgskaya-oblast-s/act-100557127 (дата обращения: 23.05.2019); Приговор Белебеевского городского суда Республики Башкортостан от 20 июня 2012 г. по уголовному делу № 1-111/2012. URL: https://rospravosudie.com/court-belebeevskij-gorodskoj-sud-respublika-bashkortost-an-s/act-106616429 (дата обращения: 23.05.2019); Приговор Промышленного районного суда г. Самары от 22 апреля 2016 г. по уголовному делу № 1-219/2016. URL: https://rospravosudie.com/court-promyshlennyj-rajonnyj-sud-g-samary-samarskaya-oblast-s/act-524031536 (дата обращения: 23.05.2019).

выхода в сеть Интернет и к информации, хранящейся в указанной сети[146].

Поскольку общественная опасность неправомерного доступа к цифровой информации близка по своей сути и общественной опасности перехвату цифровой информации в пространстве и в связи с отсутствием в УК РФ нормы, предусматривающей ответственность за перехват цифровой информации, предлагается включить упоминание о данном деянии в наименование ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ и в диспозицию ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, изложив ее в следующей авторской редакции:

> *«Статья 272. Неправомерный доступ к охраняемой законом цифровой информации или ее перехват*
> *1. Неправомерный доступ к охраняемой законом цифровой информации, а равно незаконный ее перехват, если это деяние повлекло уничтожение, блокирование, модификацию, копирование цифровой информации либо ознакомление с ней, нарушение работы информационно-телекоммуникационных устройств, их систем и сетей,– наказывается…»* (далее по тексту УК РФ).

В примечании 3 к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ предлагаем дать определение понятия «перехват цифровой информации» в следующей редакции:

> *«Под перехватом цифровой информации понимается процесс неправомерного ее получения в пространстве».*

[146] См.: Приговор Трусовского районного суда г. Астрахани от 25 марта 2010 г. URL: http://trusovsky.ast.sudrf.ru/modules.php?id=356&name=docum_sud (дата обращения: 23.05.2019).

§ 2.2. Создание, использование и распространение вредоносных компьютерных программ

Отдельным значительным пластом в массе цифровых преступлений являются деяния, связанные с созданием, использованием и распространением вредоносных компьютерных программ.

В последние годы данный вид преступлений приобрел характер транснационального и организованного. Риску воздействия вредоносных программ оказались подвержены не только компьютеры, но и мобильные устройства. Вредоносность компьютерных программ определяется тем, что все действия совершаются без уведомления пользователя, который зачастую даже не знает о существовании таких программ[147].

Для понимания угроз от вредоносных компьютерных программ приведем анализ результатов научного исследования немецкой компании, специализирующейся на обеспечении информационной безопасности *G Data Software AG*[148], которая провела опрос более 15 тыс. интернет-пользователей в возрасте от 18 до 65 лет в 11 странах мира. Почти все опрошенные пользователи (93 %) во всем мире убеждены в том, что вредоносные компьютерные программы оказывают заметное воздействие на их персональные компьютеры. Так, более 45 % всех опрошенных полагают, что в случае заражения вредоносным компьютерным программным обеспечением компьютер сразу зависает. Почти 57 % считают, что в данном случае хотя бы одна из рабочих функций компьютера повреждена или определенное программное обеспечение перестает работать. 58 % уверены, что при заражении компьютер выдает различные всплывающие окна

[147] Ефремова М. А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ // Информационное право. 2015. № 3. С. 12.

[148] G-DATA // Свободная энциклопедия Википедия. URL: https://ru.wikipedia.org/wiki/G-DATA (дата обращения: 23.05.2019).

и издает странные звуки, и почти 57 % опрошенных считают, что компьютер начинает очень медленно работать. Менее 7,5 % думают, что в случае заражения ничего необычного не обнаруживается, хотя это и происходит в большинстве случаев[149].

Высокая степень общественной опасности создания, использования и распространения вредоносных программ и компьютерной информации обусловливает формирование законодателем данного состава преступления как формального, когда сам факт создания компьютерного вируса либо совершения иного из указанных в ч. 1 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ действий, составляющих объективную сторону этого состава, является вполне достаточным для привлечения лица к уголовной ответственности. Наступление общественно опасных последствий (уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация ее средств защиты) в данном случае значения для квалификации не имеет[150].

Наиболее распространенными видами вредоносных компьютерных программ являются компьютерные вирусы, черви, сканирующие программы, обходчики средств защиты, программы управления потоками компьютерной информации, программы-патчеры[151].

Поиск упоминания наименования ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ в текстах материалов опубликованной судебной практики судов общей юрисдикции Российской Федерации, размещенных

---

[149] 10 тезисов интернет-безопасности // Information Security / Информационная безопасность. 2011. № 6. С. 22–23.

[150] Карамнов А. Ю. Ответственность за создание, использование и распространение вредоносных компьютерных программ по действующему уголовному законодательству // Социально-экономические явления и процессы. 2012. № 11. С. 286.

[151] Александрова Н. С. Преступления в сфере компьютерной информации в российском уголовном праве // Вестник Димитровградского инженерно-технологического института. 2015. № 3. С. 115.

в открытом доступе на сайтах Государственной автоматизированной системы Российской Федерации «Правосудие» и справочно-правовой системы по судебным решениям «РосПравосудие», показал структуру указанного преступления и позволил проанализировать способы осуществления незаконных действий[152].

Основными способами осуществления незаконных действий, ответственность за которые наступает по ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ, являются использование вредоносных компьютерных программ с целью доступа к охраняемой законом компьютерной информации и хищения чужих денежных средств (64,5 %), а также распространение вредоносных компьютерных программ (25,5 %). Несколько приговоров посвящены использованию вредоносных компьютерных программ, работающих на мобильных информационно-телекоммуникационных устройствах (2 %).

Примером тому может служить дело, рассмотренное Октябрьским районным судом г. Тамбова. Из материалов дела № 1–331/10 следует, что, работая в сети Интернет, гр. Б. скопировал из указан-

[152] См., например: Приговор Завьяловского районного суда Удмуртской Республики от 29 июня 2011 г. по уголовному делу № 1–131/2011. URL: https://rospravosudie.com/court-zavyalovskij-rajonnyj-sud-udmurtskaya-respublika-s/act-101685242 (дата обращения: 23.05.2019); Приговор Орджоникидзевского районного суда г. Екатеринбурга от 23 июля 2012 г. по уголовному делу № 1–429/2012. URL: https://rospravosudie.com/court-ordzhonikidzevskij-rajonnyj-sud-g-ekaterinburga-sverdlovskaya-oblast-s/act-106337351 (дата обращения: 23.05.2019); Приговор Советского районного суда г. Томска от 21 мая 2013 г. по уголовному делу № 1–174/2013. URL: https://rospravosudie.com/court-sovetskij-rajonnyj-sud-g-tomska-tomskaya-oblast-s/act-107327401 (дата обращения: 23.05.2019); Приговор Северского городского суда Томской области от 6 апреля 2015 г. по уголовному делу № 1–117/2015. URL: https://rospravosudie.com/court-severskij-gorodskoj-sud-tomskaya-oblast-s/act-488174757 (дата обращения: 23.05.2019); Приговор Минусинского городского суда Красноярского края от 7 апреля 2016 г. по уголовному делу № 1–26/2016. URL: https://rospravosudie.com (дата обращения: 23.05.2019).

ной сети на свой персональный компьютер модифицированную программу *Radmin* с возможностью скрытой установки, позволяющую администрировать подключенными в единую сеть электронно-вычислительными машинами. Согласно заключению эксперта, в компьютере гр. Б. найден файл со сценариями скрытой негласной установки серверной части программы *Radmin*, заведомо приводящей к модификации компьютерной информации[153].

Между тем за последние 20 лет уже не раз вставал вопрос об усовершенствовании уголовного законодательства в сфере компьютерной информации. Многие ученые, занимающиеся данной проблемой, периодически предлагали различные поправки и дополнения к существующим нормам, но в основном законодатель не прислушивался к их мнению.

Таким образом, уголовное законодательство в сфере компьютерной информации почти не изменялось и не дополнялось с момента принятия УК РФ 1996 г. Лишь в декабре 2011 г. законодателем предпринята попытка усовершенствовать уголовный закон в сфере компьютерной информации, и то, как нам видится, не самая удачная.

Как представляется, после вступления в силу изменений в УК РФ в редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ[154] законодателю удалось лишь немного улучшить сложившуюся ситуацию и обеспечить укрепление информационной безопасности России уголовно-правовыми средствами.

Некоторые спорные вопросы действительно решены, однако в связи с принятием изменений появились иные вопросы, требующие тщательных толкований и разъяснений.

---

[153] См.: Приговор Октябрьского районного суда г. Тамбова от 9 июля 2010 г. по уголовному делу № 1-331/2010. URL: http://sud23.tmb.sudrf.ru/modules.php?name=information&id=1242 (дата обращения: 23.05.2019).

[154] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 420-ФЗ от 7 декабря 2011 г. // СЗ РФ. 2011. № 50. Ст. 7362.

В первую очередь необходимо отметить, что скорректировано название ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ. Теперь объектами обращения вредоносных программ служат не ЭВМ, а, вероятно, компьютеры, так как в название статьи добавилось слово «компьютерных».

Слово «вредоносные», кроме названия, нигде более в статье не встречается. Видимо, законодатель предполагал под вредоносным воздействием наступление последствий, указанных в ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ.

Видится правильным положение о том, что действие вредоносных компьютерных программ может нарушить работу средств защиты компьютерной информации[155].

Законодатель, конечно же, хотел включить данные деяния в ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ, но почему-то связал это с нейтрализацией средств защиты компьютерной информации. Нам представляется, что слово «нейтрализация» является не совсем уместным, поскольку оно не является устоявшимся понятием в русском языке и не имеет единого смыслового значения[156].

Обычно слово «нейтрализация» ассоциируют с химическими процессами, происходящими в веществе. Нейтрализация (франц. *neutralisation*, от лат. *neuter* – «ни тот, ни другой»), нейтрализация реакции, химическая реакция между веществом, имеющим свойства кислоты, и веществом, имеющим свойства основания, приводящая к потере характерных свойств обоих соединений[157].

---

[155] Бегишев И. Р. Новеллы в уголовном законодательстве об ответственности за преступления в сфере компьютерной информации // Information Security / Информационная безопасность. 2012. № 2. С. 52.

[156] Бегишев И. Р. Создание, использование и распространение вредоносных компьютерных программ // Проблемы права. 2012. № 3. С. 219.

[157] Нейтрализация // Словари и энциклопедии на Академике. URL: http://dic.academic.ru/dic.nsf/bse/166987/Нейтрализация (дата обращения: 23.05.2019).

Думается, что под словом «нейтрализация» применительно к рассматриваемому явлению можно понимать либо полное или частичное уничтожение средств защиты компьютерной информации без возможности их восстановления, либо иное блокирование средств защиты компьютерной информации. Все это приводит к мысли о неточном определении вредоносного воздействия, в результате которого происходит блокирование средств защиты компьютерной информации.

Нам представляется, что более удачным решением была бы замена слова «нейтрализация» на слово «нарушение». Следует отметить, что ранее нами предлагалось использование данной терминологии и, более того, установление ответственности за незаконное обращение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, в отдельной норме уголовного закона[158].

В редакции Федерального закона от 7 декабря 2011 г. № 420-ФЗ в ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ появился новый квалифицирующий признак, такой как причинение крупного ущерба или совершение из корыстной заинтересованности. Причем законодатель определил, что крупным ущербом в статьях гл. 28 «Преступления в сфере компьютерной информации» УК РФ признается ущерб, сумма которого превышает один миллион рублей.

Ущерб от проникновения вируса или иной вредоносной информации в компьютер, иное техническое устройство, компьютерную сеть бывает различным: от незначительного увеличения размера исходящего трафика (если внедрен вирус, рассылающий спам) до полного отказа работы сети или потери жизненно важной

[158] Бегишев И. Р. Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект // Информация и безопасность. 2010. № 2. С. 258.

информации[159]. Применительно к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ мы уже говорили, что ущерб в несколько десятков или сотен тысяч рублей для граждан или субъектов малого бизнеса, вполне может иметь фатальные последствия. Размер в сто тысяч, на наш взгляд, тоже заслуживает отнесения к крупному. Либо, возможно, указанный признак следовало бы сделать оценочным.

В ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ отражены единственные квалифицирующие признаки, оставшиеся без изменений по отношению к старой редакции УК РФ, а именно совершение группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения. Несомненно, такие признаки часто встречаются на практике, и их декриминализация привела бы к негативным последствиям.

В ч. 3 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ установлена ответственность за деяния, предусмотренные частями первой, второй или третьей данной статьи, если они повлекли тяжкие последствия или создали угрозу их наступления. Причем наказание за такие деяния определено в виде лишения свободы на срок до семи лет. Видится правильным решение законодателя о введении соответствующего признака и о тяжести его наказания. Вместе с тем термин «тяжкие последствия» в статье не раскрыт даже примерно, что представляется неудачным с позиции единообразия правоприменения. Хотя бы примерный перечень был бы очень востребован.

Крупный ущерб, тяжкие последствия или угроза их наступления в анализируемом составе, как правило, выходят за границы элек-

[159] Энгельгардт А. А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) // Lex Russica. 2014. № 11 (т. XCVI). С. 1320.

тронной информационной среды, где совершается преступление. Они, если можно так выразиться, относятся к направленности объективной стороны деяния. Соответственно обосновывается вывод, что применительно к причинной связи оценке подлежат два вида общественно опасных последствий. Первый – несанкционированные уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация ее средств защиты. Он может не отвечать признакам крупного ущерба или тяжких последствий, но непосредственно связан (например, вызывает их) с последствиями второго вида (уровня), обобщенно описанными в законе как крупный ущерб, наступление или создание реальной угрозы наступления тяжких последствий[160].

Представляется, что реализация высказанных нами предложений позволит дифференцировать ответственность за рассматриваемые преступления.

§ 2.3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей установлена в ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ. В настоящее время проблема установления уголовной ответственности за данное деяние вызывает определенные дискуссии. Рассмотрим ее с раз-

[160] Там же. С. 1316.

ных позиций и постараемся изложить авторский вариант решения указанной проблемы.

Всеобщая информатизация общества все больше влияет на нашу жизнь. В силу этого нарушения работы информационно-телекоммуникационных устройств, их систем и сетей могут привести к катастрофическим последствиям.

Рассматриваемая норма является бланкетной и отсылает, как правило, к нормативно-правовым актам, инструкциям и правилам, устанавливающим требования к средствам хранения, обработки или передачи компьютерной информации. Так как компьютерные технологии используются в различных сферах деятельности человека, то указанные правила должны быть как унифицированными, так и учитывающими особенности этих сфер[161].

Видимо, к средствам хранения, обработки или передачи компьютерной информации относятся персональные компьютеры и иные информационно-телекоммуникационные устройства, в которых компьютерная информация обращается. Исходя из этого было бы правильнее обобщить указанные средства хранения, обработки или передачи компьютерной информации и указать вместо них в названии и диспозиции ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ более широкие по содержанию «информационно-телекоммуникационные устройства, их системы и сети»[162].

---

[161] Воробьев В. В. Вопросы применения состава ст. 274 УК РФ // Вестник Коми республиканской академии государственной службы и управления. Серия «Государство и право». 2015. № 20. С. 12.

[162] Бегишев И. Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник УрФО. Безопасность в информационной сфере. 2012. № 1. С. 16.

Основываясь на понятиях, используемых в законе, регулирующем отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации, при применении информационных технологий, а также при обеспечении защиты информации, считаем такое решение оправданным.

Так, приводя понятия и механизмы государственного регулирования в соответствие с практикой применения информационных технологий, законодатель в ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[163] дает определение информационной системы и информационно-телекоммуникационных сетей.

Кроме того, термин «информационно-телекоммуникационные устройства, их системы и сети» прочно закрепился в научном обороте, используемом различными специалистами в области информационных технологий и связи.

В подтверждение данной точки зрения приведем выводы В. С. Соловьева, считающего, что для придания системности уголовному законодательству необходимо привести к единым формулировкам диспозиции и квалифицирующие признаки статей УК РФ, предусматривающих ответственность за преступления, которые возможно совершить с использованием информационно-телекоммуникационных сетей[164].

---

[163] Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 г. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

[164] Соловьев В. С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) // Криминологический журнал Байкальского государственного университета экономики и права. 2016. № 1. С. 70.

Нарушение рассматриваемых правил может выражаться в двух формах: в несоблюдении установленных правил эксплуатации либо в нарушении информационно-телекоммуникационных сетей. Так, нарушения правил эксплуатации могут заключаться в несоблюдении сроков технического обслуживания компьютеров; в некачественном проведении профилактических работ по обслуживанию компьютеров и их программ; в использовании несертифицированных программных средств и т. д[165].

На наш взгляд, для привлечения нарушителей работы информационно-телекоммуникационных устройств, их систем и сетей к уголовной ответственности по ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ требуется принять общие нормы и правила использования информационно-телекоммуникационных устройств, их систем и сетей, которые должны быть обязательными для всех[166]. В противном случае избежать оценочного подхода и, соответственно, следственно-судебных ошибок не удастся.

В. В. Воробьев подчеркивает, что основной проблемой применения данной нормы является отсутствие какой-либо системы правил и инструкций в этой области, а также процедуры их принятия и доведения до исполнителей[167].

Следует согласиться с мнением Д. И. Гончаровой о том, что под правилами эксплуатации средств хранения, обработки или передачи

---

[165] Кузнецов А. П. Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети // Правовые вопросы связи. 2007. № 2. С. 26.

[166] Бегишев И. Р. Ответственность за нарушение работы информационно-телекоммуникационных устройств, их систем и сетей // Безопасность информационных технологий. 2011. № 1. С. 74.

[167] Воробьев В. В. Вопросы применения состава ст. 274 УК РФ // Вестник Коми республиканской академии государственной службы и управления. Серия «Государство и право». 2015. № 20. С. 13.

охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования понимаются правила, установленные федеральным законом, изготовителем или организацией, учреждением либо государственным органом, предоставившим доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию определенному кругу пользователей[168].

В. Г. Степанов-Егиянц справедливо считает, что правила эксплуатации могут содержаться как в нормативно-правовых актах или в общих требованиях по технике безопасности и эксплуатации компьютерного оборудования, так и в специальных правилах, регламентирующих особые условия его использования, в первую очередь защиту обрабатываемых данных, правила использования общих ресурсов (серверов), а также некоторые технические требования: температурный режим, использование резервного электропитания и т. д. В последнем случае они устанавливаются производителями компьютерного оборудования и комплектующих. На практике на сегодняшний день порядок использования компьютеров или их сетей устанавливается их собственником[169].

По мнению А. В. Сизова, причинение крупного имущественного ущерба не следует рассматривать в качестве тяжких последствий. Он считает, что если имущественный ущерб нанесен вследствие дезорганизации информационной системы посредством преступных действий, направленных на компьютерную инфор-

---

168 Гончарова Д. И. Проблематика уголовной ответственности за нарушения правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей // Международный журнал экспериментального образования. 2014. № 6–2. С. 33.

169 Степанов-Егиянц В. Г. Новая редакция статьи 274 Уголовного кодекса РФ: проблемы и пути решения // Мониторинг правоприменения. 2014. № 2. С. 20.

мацию, то данный ущерб будет входить в понятие существенного вреда, предусмотренного ч. 1 ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ[170].

При определении тяжких последствий в каждом случае должна устанавливаться причинно-следственная связь между нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и указанными в диспозиции последствиями. Уничтожение, блокирование, модификация либо копирование компьютерной информации обязательно должны быть следствием нарушения указанных правил, а они, в свою очередь, должны быть причиной наступления тяжких последствий[171].

Представляется оригинальной позиция Н. А. Лопашенко, которая предлагает декриминализовать состав преступления, предусмотренный ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ[172]. Кроме того, еще ряд исследователей также предлагают исключить ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ. К их числу можно отнести таких

---

[170] Сизов А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. 2007. № 4. С. 28.

[171] Бегишев И. Р. Уголовная ответственность за нарушение работы цифровых устройств, их систем и сетей // Information Security / Информационная безопасность. 2010. № 5. С. 22.

[172] Лопашенко Н. А. Уголовно-правовая и криминологическая политика государства в области высоких технологий // Сборник научных трудов Межд. конф. «Информационные технологии и безопасность». Киев: Национальная академия наук Украины, 2003. С. 89–97.

исследователей, как Т. Л. Тропина[173], М. А. Зубова[174] и Д. В. Добровольский[175].

А. Ж. Кабанова также предлагает декриминализовать указанный состав преступления и перевести его в сферу регулирования административного права[176]. Думается, что такой перевод в русло административного права нецелесообразен ввиду того, что рассматриваемые последствия имеют повышенную общественную опасность и могут причинить существенный вред обществу и государству.

Одним из самых распространенных на сегодняшний день способов дистанционной дестабилизации информационно-телекоммуникационных устройств, их систем и сетей является отказ в обслуживании. Отказ в обслуживании угрожает не самой информации, а автоматизированной системе, в которой эта информация обрабатывается. При возникновении отказа в обслуживании уполномоченные пользователи системы не могут получить своевременный доступ к необходимой информации, хотя имеют на это полное право[177].

У. В. Зинина считает, что диспозиция ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ сформулирована как бланкетная, т. е. требующая обращения к конкретным правилам, что затрудняет применение

---

[173] См.: Тропина Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 11.

[174] См.: Зубова М. А. Компьютерная информация как объект уголовно-правовой охраны: автореф. дис. … канд. юрид. наук. Казань, 2008. С. 14.

[175] Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью: автореф. дис. … канд. юрид. наук. М., 2005. С. 9.

[176] Кабанова А. Ж. Преступления в сфере компьютерной информации (уголовно правовые и криминологические аспекты): автореф. дис. … канд. юрид. наук. Ростов н/Д, 2004. С. 6.

[177] Скляров Д. В. Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. С. 10.

данной статьи в полном объеме в связи с нередким отсутствием соответствующих правил[178].

Подход Е. В. Красненковой[179], предлагающей конкретизировать диспозицию рассматриваемой статьи, представляется вполне оправданным, так как он учитывает устоявшуюся сегодня терминологию в сфере информации, информационных технологий и защиты информации.

Ввиду уточнения термина, указывающего на объекты обращения цифровой информации, обосновано предложение об изложении наименования ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ и диспозиции ч. 1 ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ в следующей авторской редакции:

> *«Статья 274. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей*
> *1. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом цифровой информации, причинившее крупный ущерб, –*
> *наказывается…»* (далее по тексту УК РФ).

[178] Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном праве: автореф. дис. … канд. юрид. наук. М., 2007. С. 14.

[179] Красненкова Е. В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: автореф. дис. … канд. юрид. наук. М., 2006. С. 10.

Поскольку деяния, предусмотренные ст. 272, 273, 274, 274.1 УК РФ, представляют собой единую систему преступлений, посягающих на цифровую информацию, то гл. 28 «Преступления в сфере компьютерной информации» УК РФ предлагается назвать «Преступления в сфере обращения цифровой информации», а ст. 272, 273 и 274 УК РФ озаглавить как «Неправомерный доступ к цифровой информации или ее перехват», «Создание, использование и распространение вредоносных цифровых программ» и «Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей» соответственно.

§ 2.4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Одной из важнейших задач современной Российской Федерации является противодействие преступности в сфере цифровых технологий. Стремительное развитие информационно-телекоммуникационных технологий приводит к тому, что преступность в этой сфере осваивает все новые методы и пространства для своих противоправных деяний, причем как на международной арене, так и на территории нашей страны[180].

Научно-технические достижения и инновации в сфере информационно-телекоммуникационных технологий способствуют не только прогрессивному экономическому развитию, но и приводят к появлению новых форм преступных посягательств на информационные инфраструктуры критически важных и потенциально опасных объектов. Современные информационно-телекоммуни-

[180] Бегишев И. Р. Уголовно-правовые аспекты кибертерроризма // Правовые вопросы национальной безопасности. 2010. № 5–6. С. 34.

кационные технологии могут быть использованы как средства террора, войны и оружия.

Повышение уровня опасности рассматриваемых деяний в информационной сфере обусловливает необходимость повышения защищенности критически важных объектов информационной инфраструктуры, усиления противодействия угрозе распространения компьютерной преступности и ее крайней формы – кибертерроризма[181].

Думается, что разрушение информационной инфраструктуры критически важных и потенциально опасных объектов Российской Федерации путем неправомерного доступа к цифровой информации или внедрения в них вредоносных компьютерных программ может нанести значительный ущерб национальной безопасности, а также привести к экологической катастрофе, человеческим жертвам и иным тяжким и особо тяжким последствиям.

Однако не секрет, что сейчас многие страны работают над созданием кибероружия: вирусов, вредоносных кодов, логических и почтовых бомб. Их можно заложить в компьютерное оборудование и программы, а в случае необходимости привести в действие через информационно-телекоммуникационную сеть Интернет. Создается так называемый сетевой спецназ, сетевое ополчение. Конечно, его действия не приведут к разоружению противника и захвату его территории, но сумеют повредить в критические моменты компьютеры противника, проникнут в локальные сети его ведомств, парализуют военные коммуникации и подготовят

[181] Шерстюк В. П. Проблемы противодействия компьютерной преступности и кибертерроризму // Материалы четвертой Международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М. В. Ломоносова. 30–31 октября 2008 г. Том 1: Материалы пленарных заседаний; Материалы первой Всероссийской научно-практической конференции «Формирование устойчивой антитеррористической позиции гражданского общества как основы профилактики терроризма». М.: МЦНМО, 2009. С. 49.

почву для вторжения реальных боевых частей. Поражающее действие кибероружия по мере развития технологий будет только возрастать[182].

Говорить об акте компьютерного терроризма следует лишь тогда, когда разрушительный характер произведенного действия напрямую связан с применением компьютерных технологий и программного обеспечения. При этом неважно, направлен ли он на нарушение функционирования информационных объектов или иных систем, оказывающих влияние на жизнедеятельность общества[183].

Так, И. А. Пеньков указывает, что кибертерроризм является сегодня одним из наиболее опасных видов терроризма в целом и его последствия могут быть поистине катастрофическими. Террористические акты в Соединенных Штатах Америки 11 сентября 2001 г. и авария в энергетической системе в августе 2003 г.– наглядные тому примеры[184].

Сегодня преступники, которые специализируются на совершении преступлений с использованием высоких технологий, все чаще подвергают атакам государственные, коммерческие и иные информационно-телекоммуникационные сети.

Так, сайт газеты «Московский комсомолец» подвергся хакерской атаке, в результате которой было уничтожено все его содержимое, включая редакторский интерфейс и архив за все годы существования этого сайта. Как предполагается, атака велась с серверов, находя-

[182] Павлищев Б. Борьба с кибертерроризмом: у России и США разные подходы // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/news/11.03.2009/6436/ (дата обращения: 23.05.2019).

[183] Маслакова Е. А. Кибертерроризм как новая форма терроризма // Наука и практика. 2015. № 2. С. 81.

[184] Пеньков И. А. Основные направления борьбы с кибертерроризмом // Мир и Согласие. 2006. № 1. С. 32.

щихся в Корейской Народно-Демократической Республике, вероятно, какой-то хакерской организацией или даже спецслужбой[185].

Крайне опасными можно считать атаки, направленные на полную или частичную дестабилизацию информационных представительств органов государственной власти и местного самоуправления в информационно-телекоммуникационной сети Интернет[186].

Как подчеркнул И. С. Иванов, «сохраняется высокая интенсивность компьютерных атак на критически важные объекты инфраструктуры России. По данным спецслужб, ежегодно выявляется около 700 тыс. попыток проведения атак через информационно-телекоммуникационную сеть Интернет на официальные информационные ресурсы органов государственной власти России, из них около 80 тыс. атак – на официальное интернет-представительство Президента Российской Федерации»[187].

Помимо информационных представительств указанных органов в сети Интернет, к уязвимым местам их информационно-телекоммуникационных систем относятся:

– протоколы передачи цифровой информации;

– программное обеспечение в коммуникационном оборудовании;

– хранилища и базы данных с удаленным доступом;

– зарубежное цифровое коммуникационное оборудование, используемое в режиме черного ящика в первичных каналах связи и локальных вычислительных сетях с удаленным доступом без

---

185 Тяжлов И. Хакеры уничтожили сайт «Московского комсомольца» // Коммерсантъ. 2009. № 227. С. 6.

186 Бегишев И. Р. Безопасность России: вопросы противодействия кибертерроризму // Фонд содействия научным исследованиям проблем безопасности «НАУКА-XXI». URL: http://www.naukaxxi.ru/materials/298 (дата обращения: 23.05.2019).

187 Хакеры осуществляют 700 тысяч атак в год на государственные интернет-ресурсы // Информационный портал по безопасности SecurityLab.ru. URL: http://www.securitylab.ru/news/297360.php (дата обращения: 23.05.2019).

принципиальных электрических схем и полной эксплуатационной и конструкторской документации[188].

Так, В. П. Шерстюк отмечает, что уже созданы государственные системы защиты государственной тайны и информации, системы лицензирования деятельности организаций в области защиты информации и системы сертификации средств защиты информации[189].

Следует особо отметить, что на сегодняшний день в мире несколько стран занимаются подготовкой специальных подразделений для совершения атак на информационные инфраструктуры критически важных и потенциально опасных объектов противников.

Так, глава антивирусной компании *McAfee* Дейв Ди Велт, выступая на Всемирном экономическом форуме в Давосе, сообщил, что Китайская Народная Республика, Соединенные Штаты Америки и Российская Федерация, равно как и еще несколько крупнейших в мире стран, активно занимаются созданием киберподразделений для совершения атак на информационные ресурсы потенциальных противников. Кроме того, все эти страны целенаправленно активно занимаются «интернет-шпионажем» в отношении друг друга[190].

Современные угрозы и вызовы требуют и подготовки специалистов в рассматриваемой сфере, и поиска талантов. Например, народно-освободительная армия Китайской Народной Республики устраивает общенациональные кампании в форме олимпиад

---

[188] Климов С. М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем // Известия Таганрогского государственного радиотехнического университета. 2005. № 48. С. 74.

[189] Шерстюк В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности // Информационное общество. 1999. № 5. С. 4.

[190] В мире два десятка стран занимаются кибероружием // Портал новостей высоких технологий и науки CyberSecurity.ru. URL: http://www.cybersecurity.ru/armament/ 86546.html (дата обращения: 23.05.2019).

с большими денежными призами для поиска и найма талантливых хакеров. Хакер Тан Дайлин как победитель одной из таких олимпиад получил от командования военного округа предложение поучаствовать в учениях по атакам и защите компьютерных сетей. Позднее его с товарищами включили в команду на общенациональном уровне. Утверждается, что его команда развернула атаки против американских правительственных ведомств и выкачала оттуда тысячи не секретных, но важных документов[191].

Следует отметить, что в Европейском союзе уже давно организовываются и проводятся крупномасштабные национальные, международные и транснациональные киберучения. В целом киберучения способствуют повышению уровня специальной подготовки руководящего состава и подчиненных органов управления, сил и средств кибербезопасности для надлежащего обеспечения устойчивого функционирования критически важных объектов национальной инфраструктуры в условиях информационно-технических воздействий вероятного противника[192].

Сегодня в нашей стране вопросам подготовки киберспециалистов уделяется огромное внимание. Так, в соответствии с п. 45 «Концепции противодействия терроризму в Российской Федерации», утвержденной Президентом Российской Федерации 5 октября 2009 г., приоритетным направлением кадровой политики государства является подготовка специалистов в специфических областях противодействия терроризму, в том числе кибертерроризму[193].

Изложено, что информационно-телекоммуникационные технологии могут быть использованы и как разновидность оружия.

---

[191] Ревич Ю. Вся правда о кибервойнах // Новая газета. URL: http://www.novayagazeta.ru/society/41482.html (дата обращения: 23.05.2019).

[192] Петренко А. А., Петренко С. А. Киберучения. Методические рекомендации ENISA // Вопросы кибербезопасности. 2015. № 3. С. 9.

[193] Концепция противодействия терроризму в Российской Федерации (утв. Президентом Российской Федерации 5 октября 2009 г.) // Российская газета. 2009. № 198.

Во многих странах разрабатываются стратегии ведения виртуальной войны, между ними идет гонка кибервооружений, которые создаются с целью вывода из строя государственных компьютерных сетей и объектов жизнеобеспечения[194].

Вопросами противодействия таким преступлениям обеспокоено все мировое сообщество, ведь атаки против объектов жизнеобеспечения и обороны страны могут привести к глобальным жертвам и разрушениям[195].

Одним из негативных последствий бурного развития информационно-коммуникационных технологий и сети Интернет является появление новых форм международных конфликтов, включая информационные и сетевые войны[196].

Проблема усугубляется еще и тем, что многие страны начали не только создавать подразделения, отражающие возможные преднамеренные посягательства на их критическую информационную инфраструктуру, но и тем, что они начали активно готовить специалистов для ведения информационных войн[197].

Как справедливо отмечает А. В. Крутских, в современном мире происходит постепенная «информатизация» вооруженных сил и «интеллектуализация» традиционных вооружений. Информационное оружие становится важным элементом военного потенциала государства[198].

---

[194] Панасенко А. Мы стоим на пороге кибернетических войн // Информационно-аналитический центр Anti-Malware.ru. URL: http://www.anti-malware.ru/node/1987 (дата обращения: 23.05.2019).

[195] Бегишев И. Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов // Информационная безопасность регионов. 2010. № 1. С. 10.

[196] Сурма И. В. Цифровая дипломатия в мировой политике // Государственное управление. Электронный вестник. 2015. № 49. С. 220.

[197] Бегишев И. Р. Информационное оружие как средство совершения преступлений // Информационное право. 2010. № 4. С. 24.

[198] Крутских А. В. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы. 2007. № 13. С. 28.

Учитывая, что информационное пространство все больше становится ареной противостояния, критически важно международно-правовое регулирование правоотношений в информационно-телекоммуникационной сети[199]. Так, В. В. Качалов считает, что в целях совершенствования международно-правового регулирования терроризма необходима разработка специальных международных договоров, направленных на противодействие новым террористическим проявлениям. Например, представляется, что требует такой отдельной международной регламентации противодействие кибертерроризму, т. е. терроризму с использованием возможностей компьютерных систем, сетей или данных, так как, к сожалению, текст Конвенции о компьютерных преступлениях[200] не затрагивает непосредственно вопросы противодействия терроризму[201]. Указанная проблема актуализирует необходимость проведения анализа и переосмысления современной политики противодействия кибертерроризму[202], особо серьезных преступлений, связанных с жестокостью и совершением актов насилия с помощью высоких технологий[203].

---

[199] Борисов С. В., Васнецова А. С., Жафяров А. Г. К вопросу о противодействии кибертерроризму и киберэкстремизму // Вестник Академии Генеральной прокуратуры Российской Федерации. 2015. № 1. С. 51.

[200] Конвенция о компьютерных преступлениях от 23 ноября 2001 г. (ETS № 185) // Совет Европы. Бюро договоров. URL: http://www.coe.int/it/web/conventions/home/-/conventions/rms/0900001680081580 (дата обращения: 23.05.2019).

[201] Качалов В. В. Международно-правовое регулирование противодействия терроризму // Вестник экономической безопасности. 2016. № 1. С. 90.

[202] Клименский М. М. Международно-правовое регулирование противодействия терроризму // Сборники конференций НИЦ Социосфера. 2014. № 33. С. 23.

[203] Денисов Н. Л., Ромашкина Н. Ю. Классификация современных киберпреступлений // Уголовное право и информатизация преступности: проблемы теории, практики и преподавания: сборник статей по материалам Всерос. науч. конф. М.: Издательский дом «Юриспруденция», 2018. С. 254.

Обеспечение международной информационной безопасности состоит в необходимости расширения связей между государствами с целью выработки общих усилий по борьбе с использованием информационно-коммуникационных технологий:

– для осуществления враждебных действий и актов агрессии;

– в террористических и экстремистских целях;

– в преступных целях;

– в качестве инструмента вмешательства во внутренние дела суверенных государств[204].

Кроме того, прогрессивное развитие государств возможно только при условии наиболее полного обеспечения надлежащего уровня информационной безопасности и противодействия источникам угроз в информационной сфере. В условиях глобализации и жесткой международной конкуренции информационная безопасность приобретает первостепенное значение в обеспечении национальных интересов государств, а успешное сотрудничество стран в этом вопросе играет одну из решающих ролей[205].

Следует отметить, что международное законодательство в сфере борьбы с киберпреступностью не столь развито, как хотелось бы. Так, на повестку дня двенадцатого Конгресса ООН по предупреждению преступности и уголовному правосудию был поставлен вопрос противодействия киберпреступности. После его обсуждения была принята резолюция, в п. 31 которой было определено, что законодательство о киберпреступности в настоящее время разрабатывается в основном на национальном и региональном уровнях. В отличие от

---

[204] Казарин О. В., Скиба В. Ю., Шаряпов Р. А. Новые разновидности угроз международной информационной безопасности // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2016. № 1. С. 55.

[205] Агапов П. В., Ефремова М. А. Международно-правовые основы обеспечения информационной безопасности участников содружества независимых государств // Юридическая наука и правоохранительная практика. 2015. № 1. С. 182.

технической стандартизации процедур передачи данных, которые сегодня одинаковы повсюду в мире, никаких глобальных усилий по согласованию законодательства о киберпреступности до сих пор не предпринималось[206].

Ведущим способом борьбы с данной формой преступности следует считать использование норм национального уголовного права, которое в наибольшей степени соответствует текущему состоянию преступности в этой сфере, а также интересам государства и общества[207].

Информационная безопасность в ее уголовно-правовой трактовке представляет собой динамичную открытую систему общественных отношений, обеспечивающих реализацию интересов личности, общества и государства в информационной сфере[208]. При этом предложено выделить ее в качестве самостоятельного объекта уголовно-правовой охраны, она может выступать как основным, так и дополнительным объектом посягательства[209].

Представляется, что состояние информационной безопасности и формирование «иммунитета» к киберпреступности зависит не только от уровня развития специального законодательства,

---

[206] Последние тенденции в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе применительно к киберпреступности // Секретариат Организации Объединенных Наций. URL: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF. 213_9/V1050384r.pdf (дата обращения: 23.05.2019).

[207] Степанов-Егиянц В. Г. Безопасное обращение компьютерной информации и проблемы международного правотворчества // Историческая и социально-образовательная мысль. 2015. № 2. С. 168.

[208] Ефремова М. А. К вопросу об уголовно-правовом обеспечении информационной безопасности // Вестник Тверского государственного университета. Серия: Право. 2013. № 35. С. 90.

[209] Ефремова М. А. Информационная безопасность как объект уголовно-правовой охраны // Информационное право. 2017. № 5. С. 21.

но и от уровня грамотности населения в сфере ИТ-технологий. Соответственно, в основе причинного комплекса совершения преступлений в рассматриваемой сфере лежит как отсутствие рациональных и эффективных инструментов для предотвращения неправомерного обращения с информацией, так и неумение пользоваться уже имеющимися механизмами защиты, непонимание уязвимости информационных ресурсов, чем, разумеется, с успехом пользуется криминалитет. Тем не менее степень риска нарушения прав и законных интересов различных субъектов существенно повышается в связи с внедрением автоматизированных информационных систем и новых технологий управления и обработки информации. Круг преступлений в информационной сфере, безусловно, не ограничивается лишь деяниями, закрепленными в гл. 28 УК РФ, поскольку сама компьютерная (цифровая) информация и физические ее носители и средства передачи могут выступать не только объектами преступных посягательств, но и средствами их совершения, в результате чего может быть поставлена под угрозу общественная безопасность, причинен крупный экономический ущерб, вред жизни и здоровью людей[210].

Как отметил В. Коржов, в современной войне важно добиться технологического и информационного превосходства, для чего уже недостаточно иметь хорошо вооруженную армию. Нужно еще сохранить возможности управления ею и координации действий ее подразделений. В то же время основная задача современной войны заключается уже не в том, чтобы вывести из строя боевые силы противника, а в том, чтобы подавить его системы управления. А этой цели можно добиться без использования дорогого оружия, но с помощью более дешевых высоких технологий общего назначения, которые к тому же можно использовать не только в военное,

[210] Козаев Н. Ш. Некоторые проблемы обеспечения информационной безопасности уголовно-правовыми средствами // Вестник СевКавГТИ. 2014. № 16. С. 164.

но и в мирное время. Поэтому некоторые иностранные государства взяли курс на ведение информационных войн[211].

В то же время в составе Вооруженных сил Российской Федерации созданы войска информационных операций. Их главное предназначение – защита российских военных систем управления и связи от кибертерроризма и надежное закрытие проходящей по ним информации от вероятного противника[212].

Кроме того, на Федеральную службу безопасности Российской Федерации возлагаются полномочия по созданию государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации – информационные системы и информационно-телекоммуникационные сети, находящиеся на территории Российской Федерации и в дипломатических представительствах и консульских учреждениях Российской Федерации за рубежом[213].

Обычно под информационной войной понимают целенаправленные действия, предпринятые для достижения информационного превосходства путем нанесения ущерба информации, информационным процессам и информационным системам противника при одновременной защите собственной информации, информационных процессов и систем[214].

---

[211] Коржов В. Электронное правительство против кибертеррористов // Computerworld Россия. 2008. № 4.

[212] Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций // ТАСС: информационное агентство России. URL: http://tass.ru/politika/1179830 (дата обращения: 23.05.2019).

[213] См.: О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента Российской Федерации № 31с от 15 января 2013 г. // СЗ РФ. 2013. № 3. Ст. 178.

[214] Левин В. И. История информационных технологий. М.: Бином. Лаборатория Знаний, 2009. 336 с.

Ряд специалистов говорит о необходимости ответственности лиц, способствующих распространению идеологии терроризма в информационно-телекоммуникационном пространстве. Так, Т. А. Полякова и О. В. Тульская считают, что в законодательстве Российской Федерации для пресечения распространения противоправной информации целесообразно предусмотреть возможность аннулирования лицензии провайдера, размещающего сайты террористического или экстремистского характера[215].

Думается, что такие действенные меры помогут остановить распространение идеологии терроризма в сети Интернет.

Как отмечает Д. Фролов, «Уже сегодня кибертерроризм может нанести значительно больший вред, чем обычное взрывное устройство. Например, выход из строя электронных систем управления войсками и оружием может привести к непредсказуемым последствиям»[216].

Термин «кибертерроризм» образован путем соединения двух понятий: «киберпространство» и «терроризм». Понятие «киберпространство» есть не что иное, как информационное пространство.

В ст. 3 «Основные понятия» Федерального закона от 6 марта 2006 г. № 35-ФЗ «О противодействии терроризму» «терроризм» определяется как идеология насилия и практика воздействия на принятие решения органами государственной власти, органами местного самоуправления или международными организациями, связанные с устрашением населения и (или) иными формами противоправных насильственных действий[217].

---

[215] Полякова Т. А., Тульская О. В. Правовые проблемы установления ответственности за использование информационно-телекоммуникационных систем в террористических и экстремистских целях // Проблемы правовой информатизации. 2006. № 2. С. 36.

[216] Сегодня кибертерроризм может нанести значительно больший вред, чем обычное взрывное устройство // ФСБ России: офиц. сайт. URL: http://www.fsb.ru/fsb/comment/remark/single.htm!id=10310485@fsbComment.html (дата обращения: 23.05.2019).

[217] О противодействии терроризму: Федеральный закон № 35-ФЗ от 6 марта 2006 г. // СЗ РФ. 2006. № 11. Ст. 1146.

В соответствии с п. 5 Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов[218], под «критически важными объектами» следует понимать объекты, нарушение (или прекращение) функционирования которых приводит к потере управления экономикой страны, субъекта или административно-территориальной единицы, ее необратимому негативному изменению (или разрушению) или существенному снижению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени, а под «потенциально опасными объектами инфраструктуры Российской Федерации» понимают объекты, на которых используют, производят, перерабатывают, хранят, эксплуатируют, транспортируют или уничтожают радиоактивные, пожаровзрывоопасные и опасные химические и биологические вещества, а также гидротехнические сооружения, создающие реальную угрозу возникновения источника кризисной ситуации.

Следует отметить, что вопрос отнесения информационной инфраструктуры к критически важным и потенциально опасным объектам Российской Федерации остается пока открытым.

В. А. Васильев также высказывает мнение о необходимости определения законодательного механизма отнесения рассматриваемых объектов к критически важным[219].

Депутатами Государственной Думы Российской Федерации еще в 2006 г. зарегистрирован и направлен Председателю законопроект

---

[218] Об одобрении Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов: Распоряжение Правительства Российской Федерации № 1314-р от 27 августа 2005 г. // СЗ РФ. 2005. № 35. Ст. 3660.

[219] Васильев В. А. Проблемы развития законодательства в сфере борьбы с киберпреступностью // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/articles/vasil06 (дата обращения: 23.05.2019).

№ 340741–4 «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры». Целью данного законопроекта являлось установление организационно-правовых особенностей обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры различных видов собственности и установление форм и методов государственного регулирования ее обеспечения[220].

Данный законопроект так и не был принят, так как в марте 2008 г. был снят с рассмотрения Государственной Думы в связи с отзывом субъектом права законодательной инициативы[221]. По нашему убеждению, его снятие политически спровоцировано большим количеством программных продуктов от корпорации *Microsoft*, используемых на критически важных объектах информационной инфраструктуры России, так как они бы не смогли так успешно реализовывать свои программные продукты в этой сфере и понесли бы огромные финансовые убытки.

По нашему мнению, необходимо было дать дорогу этому законопроекту и рассмотреть его как можно быстрее, так как недостаточное правовое регулирование вопросов отнесения объектов информационной инфраструктуры к критически важным негативно сказывается на обеспечении информационной безопасности Российской Федерации[222].

---

[220] См.: Законопроект № 340741-4 «Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры» // Автоматизированная система обеспечения законодательной деятельности Государственной Думы Российской Федерации. URL: http://asozd2. duma.gov.ru/main.nsf/(Spravka)?OpenAgent&RN=340741-4&11 (дата обращения: 23.05.2019).

[221] Там же.

[222] Бегишев И. Р. Открытое ПО: вопросы права, безопасности и последствий // Information Security / Информационная безопасность. 2011. № 4. С. 29.

Сегодня наиболее опасными считаются атаки на объекты критической информационной инфраструктуры, в том числе на координирующие серверы *IoT*-устройств[223]. Опасность таких действий заключается в возможной дестабилизации не только отдельного предприятия, но и субъекта Федерации, федерального округа или страны в целом, поскольку они могут привести к существенным повреждениям объектов жизнеобеспечения, транспорта и связи, энергетики и промышленности, к экологическим катастрофам и гибели людей. Во многих случаях положение усугубляется недостаточной защищенностью указанных объектов.

Особое внимание со стороны государства должно быть сосредоточено на предотвращении действий, направленных на развязывание против него информационных войн, нацеленных на дестабилизацию системы национальной безопасности.

В качестве информационного оружия могут выступать совершенно различные средства: высокоточное оружие для поражения органов управления или отдельных радиоэлектронных средств, средства радиоэлектронной борьбы, источники мощного электромагнитного импульса, программные вирусы и др. В качестве критерия отнесения к разряду информационного оружия может рассматриваться только эффективность того или иного устройства при решении задач информационной войны.

Представляется, что силы и средства противника, применяющего информационное оружие, направлены в первую очередь на дестабилизацию критической информационной инфраструктуры Российской Федерации.

В полной мере осознавая высокую степень опасности умышленных воздействий в информационно-телекоммуникационной среде, многие страны старательно пытаются закрыть существующие ныне

[223] Бегишев И. Р. Некоторые аспекты информационной безопасности технологии блокчейн // Information Security / Информационная безопасность. 2018. № 6. С. 18.

бреши в кибероборонe, создавая специальные правоохранительные органы и их подразделения, в задачи которых входит противодействие посягательствам на информационные инфраструктуры своих объектов.

Так, Министерство обороны Соединенных Штатов Америки вместе с зарубежными партнерами собирается направить усилия на создание средств защиты сетей, их функциональных возможностей и обеспечения надежности в киберпространстве[224]. В свою очередь, власти крупнейших мировых государств создают подразделения киберспецназа.

Проблема усугубляется еще и тем, что многие страны начали не только создавать подразделения, отражающие возможные преднамеренные посягательства на их критическую информационную инфраструктуру, но и активно готовить специалистов по боевому применению информационно-телекоммуникационных систем в условиях войны или вооруженных конфликтов.

А. И. Маляров пришел к аналогичным выводам в своем исследовании. Он также указывает на важность существующей проблемы и отмечает, что Соединенные Штаты Америки в рамках специальной программы создали самый крупный в мире отряд программистов-хакеров – Объединенное функциональное подразделение для ведения сетевой войны. Основным предназначением этого подразделения является ведение бесконтактной сетевой войны (проведение кибератак) против информационной составляющей противоборствующего государства. Военным ведомством Китайской Народной Республики также ведется подготовка персонала по боевому применению информационно-телекоммуникационных систем. В частности, в настоящее время в народно-освободительной армии Китайской Народной Республики уже созданы специаль-

[224] Конышев В. Н., Сергунин А. А. Новая военная доктрина Барака Обамы и национальные интересы России // Национальные интересы: приоритеты и безопасность. 2012. № 14. С. 6.

ные резервные полки, а также спецбатальоны, укомплектованные указанными специалистами. Подготовкой персонала по боевому применению информационно-телекоммуникационных систем также занимаются Корейская Народно-Демократическая Республика и Исламская Республика Иран[225].

Мы солидарны с С. М. Ивановым и О. Г. Томило, которые считают, что для успешного противодействия кибертерроризму необходимо создание национальных подразделений по борьбе с киберпреступностью и международного контактного пункта по оказанию помощи для реагирования на транснациональные компьютерные инциденты[226]. Аналогичной позиции придерживаются К. А. Пшенко и П. К. Анисимов[227].

Революционные темпы развития информационно-телекоммуникационных сетей расширяют возможности их использования в различных видах преступной и иной противоправной деятельности. Рост количества пользователей информационно-телекоммуникационной сети Интернет способствует не только совершению в отношении них преступлений, но и возможности их участия в преступной деятельности, в том числе в ее организованных формах. Отсутствие физических границ в сети Интернет позволяет использовать ее в целях совершения транснациональных преступлений[228].

---

225 Маляров А. И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. … канд. юрид. наук. Краснодар, 2008. С. 15.

226 Иванов С. М., Томило О. Г. Международно-правовое регулирование борьбы с кибертерроризмом // Право и безопасность. 2013. № 3–4. С. 85.

227 Пшенко К. А., Анисимов П. К. Кибертерроризм – угроза международной безопасности // Национальная безопасность и стратегическое планирование. 2015. № 3. С. 96.

228 Антонов О. Ю. Выявление дополнительных эпизодов и новых видов порно-сексуальной преступной деятельности, совершаемой с использованием информационно-телекоммуникационных сетей // Расследование преступлений: проблемы и пути их решения. 2017. № 3 (17). С. 170.

Транснациональный характер посягательств в информационной сфере, обусловленный техническими возможностями, открывает широкие возможности для развития теневого бизнеса[229], способен нанести непоправимый ущерб экономике сразу нескольких государств[230].

Представляется, что Россия не должна оставаться в стороне от этих тенденций. Возможно, создание отечественного единого специального федерального органа исполнительной власти в области расследования и предупреждения преступлений в цифровой сфере, включая обеспечение безопасности объектов критической информационной инфраструктуры, а также воздействие на информационные инфраструктуры противника, тоже имело бы смысл.

Такое ведомство могло бы называться, например, Федеральной службой информационной безопасности Российской Федерации и объединять имеющиеся на сегодняшний день силы, средства, интеллектуальный и практический потенциал специальных служб и правоохранительных органов России, связанных с обеспечением информационной безопасности, главным образом таких, как Федеральная служба безопасности, Федеральная служба по техническому и экспортному контролю, Служба специальной связи и информации Федеральной службы охраны Российской Федерации, Бюро специальных технических мероприятий Министерства внутренних дел России и ряд других[231].

---

[229] Хисамова З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: автореф. дис. … канд. юрид. наук. Краснодар, 2016. С. 3.

[230] Хисамова З. И. Способы легализации (отмывания) доходов, полученных преступным путем, с использованием информационно-телекоммуникационных технологий // Вестник Краснодарского университета МВД России. 2017. № 2 (36). С. 84.

[231] Бегишев И. Р. Федеральная служба информационной безопасности Российской Федерации: миф или реальность? // Information Security / Информационная безопасность. 2016. № 6. С. 15.

Между тем в настоящее время в действующей системе правоохранительных органов России в сфере обеспечения информационной безопасности имеется ряд пробелов, таких как разрозненность и дублирование функций, бессистемность и несогласованность правоприменительных органов, различный внутриведомственный подход каждого правоохранительного органа, частое затягивание решений проблем ввиду необходимости согласования и т. д.

Анализ актуальности рассматриваемых в работе проблем показывает, что существенной профилактической мерой улучшения сложившейся ситуации, по аналогии с развитием подобных структур в развитых странах, является объединение сил и средств специальных служб в целях комплексного обеспечения необходимого уровня защищенности информационных инфраструктур.

Также необходимо отметить, что действия против киберпреступности должны быть направлены в первую очередь на предупреждение подобных преступлений путем целенаправленного воздействия на потоки информации.

Таким образом, кибертерроризм есть не что иное, как определенный вид терроризма, направленный на дестабилизацию, устрашение и иное воздействие на принятие решений органами государственной власти и местного самоуправления с использованием современных информационно-телекоммуникационных технологий, связанных с критически важными и потенциально опасными объектами информационной инфраструктуры России.

В Российской Федерации этот термин не получил пока легального закрепления, хотя о нем уже спорят юристы-практики и теоретики, изучающие проблему киберпреступности, а также технические специалисты, которые занимаются пресечением или предотвращением угроз вторжения, в том числе актов кибертерроризма. По мнению большинства экспертов, наибольшая угроза со стороны кибертеррористов таится в предоставляемых им возможностях сети Интернет для осуществления кибератак, направленных

на уязвимые звенья критической инфраструктуры, в первую очередь транспорта и энергетики[232].

Основной причиной отсутствия четкой формулировки этого, безусловно, актуального вида преступлений являются пробелы в законодательстве многих стран. С одной стороны, это объяснимо, ведь первые исследования проблемы киберпреступности и разработка мер стали производиться относительно недавно[233]. С другой стороны, интересы сохранения государственной тайны препятствуют свободному движению информации о соответствующих явлениях.

Поскольку законодательно кибертерроризма в нашей стране нет, то и меры противодействия данному виду преступности не развиты на должном уровне[234]. Необходимо отметить, что, несмотря на усилия, прикладываемые международным сообществом, и многочисленные декларации, понятие «кибертерроризм» законодательно закреплено лишь в двух государствах – в США и на Украине[235].

Т. Л. Тропина также отмечает, что первым шагом в борьбе с киберпреступностью и ее опаснейшей разновидностью – кибертерроризмом – должно стать создание корректного понятийного аппарата. Многие средства массовой информации употребляют термин «кибертерроризм» весьма некорректно, создавая путаницу

---

[232] Беспалов В. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом // Центр исследования компьютерной преступности. URL: http://www.crime-research.ru/articles/ceberteror (дата обращения: 23.05.2019).

[233] Кошечкина Е. А. К вопросу о противодействии кибертерроризму в Российской Федерации и Республике Узбекистан // The Newman in Foreign Policy. 2017. № 39 (83). С. 42.

[234] Кошечкина Е. А. К вопросу о проблемах законодательства в сфере кибертерроризма // Омский научный вестник. Серия Общество. История. Современность. 2017. № 4. С. 104.

[235] Там же. С. 100.

в понятиях, ставя знак равенства между понятиями «хакер» и «кибертеррорист». Вряд ли это можно счесть правильным. По мнению исследователя, терроризм – это преступление, но не каждое преступление есть терроризм, точно так же как кибертеррориста, как правило, можно назвать хакером, но не всякий хакер совершает теракты в киберпространстве или с помощью компьютера[236].

Г. А. Шагинян, рассматривая характер и особенности актов кибертерроризма, выдвигает мнение о необходимости организационной и в первую очередь финансовой поддержки масштабных научных исследований феномена кибертерроризма в следующих направлениях: разработка единого понятийного аппарата, включая универсальное определение кибертерроризма с целью его дальнейшей кодификации в уголовном законодательстве страны; совершенствование критериальной основы оценки безопасности информационных технологий, разработка новых конструктивных моделей тестирования, верификации средств защиты сложно организованных компьютерных систем, формирование доказательной базы их гарантированной защищенности; совершенствование системы подготовки кадров в области информационной безопасности, причем как специалистов по техническим аспектам защиты информации, так и юристов со специализацией «расследование компьютерных преступлений»[237].

Как справедливо указывает В. А. Мазуров, арсенал компьютерных террористов – различные вирусы, логические бомбы (команды, встроенные заранее в программу и срабатывающие в нужный

[236] Тропина Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Киев: Национальная академия наук Украины, 2003. С. 181.

[237] Шагинян Г. А. Антитеррористическая информационная политика Российского государства: автореф. дис. … канд. полит. наук. Краснодар, 2006. С. 24.

момент). Современные террористы используют сеть Интернет в основном как средство пропаганды, передачи информации, а не как новое оружие. В настоящее время существует мало систем, которые можно назвать абсолютно защищенными[238].

В.И. Федулов, исходя из правового понятия «терроризм» и сочетания его с дефиницией «виртуальное пространство», выводит следующее определение: «Кибертерроризм – это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами»[239].

Г.А. Шагинян в рамках исследования проблемы антитеррористической информационной политики российского государства высказывает мнение о необходимости внесения кибертерроризма в разряд уголовных преступлений и создания всеобъемлющей правовой базы для борьбы с данным явлением. Важным является продолжение работы в рамках международных организаций по унификации национальных законодательств в области борьбы с киберпреступностью и кибертерроризмом, и с этой целью необходима подготовка на национальном уровне конкретных предложений по созданию соответствующего международного документа[240]. С последним сложно не согласиться.

Следует поддержать мнение Н.А. Чернядьевой, которая считает, что кибертерроризм обладает исключительно опасным международным потенциалом, требуется скорейшее создание международно-правовых норм, обеспечивающих глобальную защиту сети

---

[238] Мазуров В. А. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции // Вестник ТГУ. 2007. № 1. С. 152.

[239] Федулов В. И. Компьютерный терроризм как инновация современного высокотехнологичного общества // Вестник МГОУ. Серия «Юриспруденция». 2007. № 1 (т. 2). С. 105.

[240] См.: Шагинян Г. А. Указ. раб. С. 24.

Интернет и иных информационных сетей от киберпреступлений в целом и от кибертерроризма в частности[241].

Д. А. Ковлагина[242] определяет кибертерроризм как составляющую часть информационного терроризма, а Т. М. Лопатина[243] относит информационный терроризм к одному из видов терроризма. С данным мнением также сложно не согласиться.

Предполагается, что мерами уголовно-правового противодействия кибертерроризму можно добиться существенного улучшения состояния защищенности критически важных и потенциально опасных объектов информационной инфраструктуры Российской Федерации.

Мнения исследователей по данному поводу можно разделить на два основных направления. Так, одна группа исследователей проблемы кибертерроризма полагает, что кибертерроризм подпадает под действие ст. 205 «Террористический акт» УК РФ и не требует включения в уголовный закон еще одной нормы. Например, Д. Б. Фролов считает, что в ст. 205 «Террористический акт» УК РФ налицо все признаки терроризма: и политическая окраска, и совершение деяний с целью создания атмосферы страха, напряженности, паники, и принцип публичности (четко выделяющий эту категорию преступлений из остальных разновидностей киберпреступности), и направленность не на конкретных лиц (в отличие от других видов преступлений), а на неопределенный круг граждан, становящихся жертвой кибертеррора. Только указанные деяния кибертеррориста носят характер не взрыва, поджога, а «иных действий». И для того чтобы кибертеррористов можно было привлекать к уголовной от-

---

[241] Чернядьева Н. А. О международных подходах правового регулирования борьбы с кибертерроризмом // Информационное право. 2016. № 2. С. 29.

[242] См.: Ковлагина Д. А. Информационный терроризм // Вестник Саратовской государственной юридической академии. 2013. № 6. С. 183.

[243] См.: Лопатина Т. М. Новые виды современной террористической деятельности // Современное право. 2012. № 4. С. 123.

ветственности по этой статье, не нужно даже вносить в эту статью поправки, достаточно дать ей более широкое толкование[244].

Другая группа исследователей видит решение данной проблемы в выделении в рамках ст. 205 «Террористический акт» УК РФ отдельного пункта, который бы усиливал уголовную ответственность за совершение террористического акта с использованием ЭВМ (компьютеров), информационных систем и телекоммуникационных сетей, связанных с критическими элементами инфраструктуры. Так, Е. С. Саломатина предлагала дополнить ч. 2 ст. 205 «Террористический акт» УК РФ пунктом «г» следующего содержания: «Те же деяния, совершенные с использованием ЭВМ (компьютеров), информационных систем и телекоммуникационных сетей, связанных с критическими элементами инфраструктуры»[245].

Отметим точку зрения С. В. Помазана, который указывает, что в проекте Федерального закона «О противодействии терроризму» приведено наиболее удачное определение терроризма: «…насилие или угроза его применения в отношении физических лиц, уничтожение (повреждение) или угроза уничтожения (повреждения) имущества либо других материальных объектов, незаконное вмешательство или угроза незаконного вмешательства в информационные ресурсы и информационные системы, а также иные действия, создающие опасность гибели людей, причинения значительного материального ущерба либо наступления иных общественно опасных последствий и совершаемые в целях устрашения населения или оказания воздействия на принятие должностными лицами, органами государственной власти, органами местного самоуправления или международными организациями решений, обеспечивающих

[244] Фролов Д. Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом // Законодательство и экономика. 2005. № 5. С. 65.

[245] Саломатина Е. С. Перспективы развития законодательства в сфере борьбы с кибертерроризмом // Закон и право. 2009. № 1. С. 47.

удовлетворение социально-политических требований и интересов террористов»[246].

Данная формулировка, в которой уже описаны действия, направленные на незаконное вмешательство в информационные ресурсы и информационные системы, не была принята. Федеральный закон изложил определение понятия терроризма в другой редакции.

В. Н. Черкасов отмечает, что если следовать логике второй группы исследователей, то в ближайшее время придется вводить в УК РФ новые статьи, криминализирующие новые виды правонарушений: кибермошенничество, киберклевету, кибершпионаж, киберподделку, киберхалатность, киберсаботаж и т. д. до бесконечности, точнее, до исчерпания УК РФ[247].

Стоит согласиться с точкой зрения Т. М. Лопатиной, которая, рассматривая криминологические подходы к пониманию условно-цифрового вымогательства, отмечает, что «эпидемия кибервымогательства постепенно захватывает интернет-пространство и в ближайшее время может стать одной из наиболее крупных криминальных проблем»[248].

Отдельные представители науки имеют сходные позиции по отнесению «кибертерроризма» к отдельному виду преступных деяний. Так, В. И. Белоножкин указывает, что реально существующие на настоящий момент проявления так называемого кибертерроризма могут быть квалифицированы как применение информационно-телекоммуникационных сетей в процессе тер-

---

[246] Памазан С. В. Проблемы современного законодательства в сфере противодействия терроризму // Вестник Владимирского юридического института. 2006. № 1. С. 239.

[247] Черкасов В. Н. Информационная безопасность. Правовые проблемы и пути их решения // Информационная безопасность регионов. 2007. № 1. С. 10.

[248] Лопатина Т. М. Условно-цифровое вымогательство, или кибершантаж // Журнал российского права. 2015. № 1. С. 119.

роористической деятельности[249]. Ему представляется, что нужно говорить о классификации методов и технологий терроризма, а не плодить его разновидности типа биотерроризма, технологического терроризма, кибертерроризма и т. д.[250]

По нашему мнению, такой подход не только не решит проблему противодействия преступлениям в сфере высоких технологий, но только запутает работников правоохранительных органов при квалификации данных деяний, так как в основном преступные деяния, совершенные кибертеррористами, подпадают под действие гл. 28 «Преступления в сфере компьютерной информации» УК РФ. Поэтому понятие кибертерроризма в уголовном законе использовать не следует, оно должно применяться исключительно в криминологических целях, да и то очень осторожно, поскольку может трактоваться неоднозначно.

Основная опасность кибертерроризма заключается в цифровых атаках на критически важные объекты информационной инфраструктуры России. К таковым следует отнести атаки на информационно-телекоммуникационные сети правительственных, военных, медицинских, финансовых и тиных организаций в целях дезорганизации их работы и с максимально возможными пагубными последствиями для них. Данные посягательства не сводятся только к преступлению, ответственность за которое предусмотрена ст. 205 «Террористический акт» УК РФ.

Глубокое изучение технических особенностей критически важных объектов не является целью настоящего исследования. Они достаточно хорошо исследованы представителями физико-математических и технических наук. Вместе с тем некоторые сведения об особенностях критически важных и потенциально опасных

[249] Белоножкин В. И. Информационная сущность и структура терроризма // Информация и безопасность. 2007. № 4. С. 542.

[250] Там же.

объектов информационной инфраструктуры представляются вполне уместными, поскольку без них исследование не будет полным.

Так, Л. А. Шивдяков, В. М. Максимов и Ю. К. Язов[251] в своей работе отмечают ряд особенностей критически важных систем и факторов, влияющих на состояние обеспечения безопасности информации в них. К таким особенностям исследователи относят следующие.

Во-первых, все критически важные системы информационной инфраструктуры являются распределенными системами, объединяющими несколько автоматизированных систем (подсистем) центральных и периферийных подразделений организации в единую информационно-телекоммуникационную сеть. При этом нарушение функционирования какой-либо из подсистем может привести к нарушению функционирования критически важных систем информационной инфраструктуры в целом. Кроме того, имеется возможность осуществления несанкционированного доступа из одной системы в другую с реализацией угроз безопасности информации.

Во-вторых, критически важная информационная инфраструктура предназначена для автоматизации управления критически важными объектами или технологическими процессами. Срыв или нарушение такого управления может достигаться в результате невыполнения, искажения команд или программ управления, из-за недоступности или искажения данных об управляемом процессе, срыва или задержки передачи данных и команд по линиям связи, недопустимой рассинхронизации управления зависимыми технологическими процессами и др. В отличие от обычных «офисных» систем, где срыв функционирования не может привести к катастрофическим последствиям, преднамеренное нарушение

[251] Шивдяков Л. А., Максимов В. М., Язов Ю. К. Особенности критически важных систем и факторы, влияющие на состояние обеспечения безопасности информации в них // Информация и безопасность. 2010. № 2. С. 243.

выполнения функций управления в критически важной информационной инфраструктуре обусловливает возможность возникновения чрезвычайных ситуаций.

К примеру, серьезные ошибки в управлении крупными технологическими системами (объекты атомной энергетики, нефтеперерабатывающие, химические комбинаты и др.) практически всегда кроются в недооценке опасности, небрежности персонала, неинформированности населения в случае аварий и катастроф. Достаточно вспомнить чернобыльскую катастрофу, где социально-управленческие просчеты в совокупности с производственно-технологическими нарушениями привели к трагическим последствиям[252].

В-третьих, в критически важной системе информационной инфраструктуры могут устанавливаться как обычные операционные системы или прикладные программы (например, текстовые и графические редакторы, системы управления базами данных, интернет-браузеры и т.п.), широко применяемые в «офисных» компьютерных сетях, так и операционные системы реального времени и специализированное прикладное программное обеспечение. В частности, в настоящее время широко используются технологии, как правило, не исследуемые на предмет защищенности от преднамеренного воздействия.

В-четвертых, функционирующие в критически важной системе информационной инфраструктуры данные не представляют собой информацию ограниченного доступа, а для обеспечения надежности их представления из баз данных может обеспечиваться реализация функций проверки (идентификации) запросов на их представление, форматов выдаваемых данных и т.п. Как правило, такие функции реализуются системами противоаварийной защиты критически

[252] Козаев Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом: дис. … д-ра юрид. наук. Краснодар, 2016. С. 61.

важной информационной инфраструктуры. Однако при преднамеренных воздействиях обойти функции систем противоаварийной защиты возможно.

В-пятых, несмотря на наличие в подавляющем большинстве критически важных систем информационной инфраструктуры ярко выраженных функциональных подсистем, как правило, некоторые из них могут сопрягаться с подсистемой, обеспечивающей деятельность администрации организации и имеющей выход в сети общего пользования (например, сеть Интернет). Кроме того, непосредственный доступ к вычислительным и информационным ресурсам имеет большое число различных категорий пользователей, и прежде всего из обслуживающего персонала. Это создает реальные предпосылки к нарушениям безопасности критически важной информации.

В-шестых, большинство критически важных систем информационной инфраструктуры работают в непрерывном режиме и не могут быть отключены, что, как правило, исключает возможность применения инструментальных средств анализа защищенности критически важной информации в них. В этих условиях оценка состояния обеспечения безопасности информации могла бы производиться на основе данных моделирования деструктивных информационных воздействий на критически важные системы информационной инфраструктуры, что в настоящее время пока невозможно из-за отсутствия подобных моделей[253].

Приведем несколько примеров возможных сценариев атак на критически важные и особо опасные объекты информационной инфраструктуры России.

Это может быть атака в виде воздействия мощного электромагнитного импульса на информационные инфраструктуры топливно-энергетического и транспортного комплексов России, в том

[253] Там же.

числе аэропортов, железнодорожных и автовокзалов, которые способны не только дезорганизовать их работу, но и повлечь за собой гибель людей, пагубные последствия для экологии страны и т. д. Причем такие действия чрезвычайно опасны, даже если не носят террористического характера.

Думается, что к аналогичным последствиям может привести и действие вредоносных компьютерных программ, попавших в информационно-телекоммуникационную сеть вышеуказанных критически важных и потенциально опасных объектов.

Также представляется, что злоумышленник под угрозой совершения цифровых атак может шантажировать руководство объекта, региона и страны, требуя от них выполнения его указаний.

Атаки кибертеррористов могут быть направлены не только на дестабилизацию информационных структур критически важных объектов, но и на вмешательство в работу государственных автоматизированных систем. Предполагается, что, например, в результате атак на государственную автоматизированную систему «Выборы» может быть дестабилизирована политическая обстановка в стране.

Считаем, что информационно-телекоммуникационные сети государственных и муниципальных органов должны быть надежно защищены от внешних посягательств, в том числе при использовании информационно-телекоммуникационных сетей международного информационного обмена.

Так, государственным органам запрещено подключаться к информационно-телекоммуникационной сети Интернет, а если подключение все же необходимо, то производится только с использованием специально предназначенных для этого средств защиты информации, в том числе шифровальных (криптографических) средств, прошедших в установленном законодательством Российской Федерации порядке сертификацию в Федеральной службе безопасности Российской Федерации и (или) получивших под-

тверждение соответствия в Федеральной службе по техническому и экспортному контролю[254].

Кроме того, в целях противодействия угрозам информационной безопасности Российской Федерации при использовании информационно-телекоммуникационной сети Интернет на территории Российской Федерации сегмент международной компьютерной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, находящийся в ведении Федеральной службы охраны Российской Федерации, преобразован в российский государственный сегмент информационно-телекоммуникационной сети Интернет, являющийся элементом российской части сети Интернет[255].

Государство также заинтересовано в безопасности информационных инфраструктур критически важных и особо опасных объектов Российской Федерации. Так, одной из основных угроз государственной и общественной безопасности является деятельность террористических и экстремистских организаций, направленная на нарушение безопасности и устойчивости функционирования критической информационной инфраструктуры Российской Федерации[256].

Мы согласны с точкой зрения В. А. Васенина, который выделяет два основных вида противоправных действий, направленных на

---

[254] См.: О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента Российской Федерации № 351 от 17 марта 2008 г. // СЗ РФ. 2008. № 12. Ст. 1110.

[255] См.: О некоторых вопросах информационной безопасности Российской Федерации: Указ Президента Российской Федерации № 260 от 22 мая 2015 г. // СЗ РФ. 2015. № 21. Ст. 3092.

[256] См.: О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации № 683 от 31 декабря 2015 г. // СЗ РФ. 2016. № 1 (ч. II). Ст. 212.

проведение террористических актов (разрушение инфраструктуры и неправомерный доступ к компьютерной информации)[257].

Необходимо согласиться с мнением В. А. Васенина о том, что следует отличать террористические действия от действий террористов с использованием сетевых ресурсов (в том числе собственных в сети «Интернет») в целях пропаганды своих взглядов, нагнетания обстановки страха, напряженности и т. д[258].

В свою очередь, И. А. Пеньков считает, что с помощью информационно-телекоммуникационной сети Интернет террористы могут:

– разрушить инфраструктуру сетей передачи данных;

– получить НДС к информации, носящей конфиденциальный характер;

– намеренно исказить информацию в средствах массовой информации и на сайтах в целях дискредитации отдельных лиц, организаций и органов власти, неадекватного отражения действительности;

– пропагандировать экстремистские идеи и оправдывать террористическую деятельность борьбой за свободу и независимость;

– поддерживать связь между собой, отдавать приказы и распоряжения, распространять инструкции по совершению террористических актов[259].

С. В. Зарубин рассматривает проблему информационного терроризма как современного социально-политического явления. Он подчеркивает, что террористы вполне могут использовать знания

---

[257] Васенин В. А. Информационная безопасность и компьютерный терроризм // Научные и методологические проблемы информационной безопасности: сборник статей / под ред. В. П. Шерстюка. М.: МЦНМО, 2004. С. 69.

[258] См.: О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации от 31 декабря 2015 г. № 683 // СЗ РФ. 2016. № 1 (ч. II). Ст. 212.

[259] Пеньков И. А. Основные направления борьбы с кибертерроризмом // Мир и Согласие. 2006. № 1. С. 33.

хакеров в своих целях, и отмечает, что рано или поздно хакер либо сам станет кибертеррористом, либо превратится в инструмент кибертеррористов[260].

Исследователь также отмечает, что преступления в информационной сфере, в число которых входит и кибертерроризм, влекут за собой наказание существенно меньшее, чем осуществление традиционных террористических актов[261].

Бесспорной представляется точка зрения А. А. Сальникова и В. В. Ященко о необходимости разработки системы мер по мониторингу и контролю за распространением знаний и технологий, критичных с точки зрения информационной безопасности[262]. Исследователи считают, что один из основных ресурсов, требующих мониторинга,– это высококвалифицированные специалисты, обладающие знаниями в области высоконадежных методов защиты информации. Именно они являются объектом интереса работодателей, в том числе по заказам международных террористических организаций.

Постоянных усилий требует также работа по согласованию взаимоприемлемых условий функционирования сети международных центров по предупреждению и противодействию кибератакам. Необходимо выработать работоспособные механизмы обмена опытом в этой области[263].

Н. Н. Радаев предлагает концепцию повышения защищенности критически важных объектов заинтересованного субъекта от терро-

---

[260] Зарубин С. В. К вопросу об оценке эффективности мероприятий по противодействию информационному терроризму // Вестник Воронежского института МВД России. 2008. № 4. С. 123.

[261] Там же.

[262] Сальников А. А., Ященко В. В. Методологические проблемы противодействия кибертерроризму // Научные и методологические проблемы информационной безопасности: сборник статей / под ред. В. П. Шерстюка. М.: МЦНМО, 2004. С. 100.

[263] Там же.

ристических действий на основе принципа равного риска, а также рациональную стратегию ее реализации. Им разработана структура показателей для оценки вероятного ущерба для заинтересованного субъекта в результате террористических действий и критерий выделения объектов, требующих первоочередной защиты[264].

Таким образом, вышеизложенное свидетельствует о сложившейся в мире и в Российской Федерации сложной ситуации в сфере обеспечения безопасности информационной инфраструктуры критически важных и потенциально опасных объектов.

Полагаем, что основными причинами, порождающими такую криминальную ситуацию и способствующими росту преступлений, посягающих на информационные инфраструктуры критически важных и потенциально опасных объектов Российской Федерации, являются:

– распространение в средствах массовой информации материалов, пропагандирующих безнаказанность кибертеррористов;

– слабая готовность правоохранительных органов и специальных служб противостоять указанным преступлениям;

– отсутствие необходимой профилактики в сфере борьбы с преступлениями, посягающими на информационные инфраструктуры критически важных и потенциально опасных объектов.

На сегодняшний день наиболее эффективным направлением противодействия преступлениям в сфере обращения цифровой информации является профилактика или предупреждение указанного вида преступности[265].

Таким образом, анализ проблем уголовной ответственности за преступления, посягающие на информационные инфраструктуры

---

[264] Радаев Н. Н. Рациональная стратегия защиты объекта. Концепция повышения защищенности критически важных объектов от технологического терроризма // Безопасность. Достоверность. Информация. 2007. № 2. С. 22.

[265] Бегишев И. Р. Меры предупреждения преступлений в сфере обращения цифровой информации // Информация и безопасность. 2011. № 3. С. 433.

критически важных и потенциально опасных объектов Российской Федерации, позволяет сделать вывод о сложившейся ситуации, представляющей реальную угрозу национальной безопасности Российской Федерации.

Остается надеяться, что законодатель учтет опасность таких преступных посягательств и в скором времени адекватно отреагирует на нависшие угрозы информационной безопасности страны.

Законодатель уже делает первые шаги в этом направлении. Он провозгласил, что в целях обеспечения государственной безопасности укрепляется режим безопасного функционирования, повышается уровень антитеррористической защищенности организаций оборонно-промышленного, ядерного, химического, топливно-энергетического комплексов страны, объектов жизнеобеспечения населения, транспортной инфраструктуры, других критически важных и потенциально опасных объектов[266].

Было бы уместным отметить, что, например, в Исламской Республике Пакистан введена смертная казнь для кибертеррористов, в результате действий которых погибли люди[267].

В условиях возрастания новых вызовов и угроз в информационной сфере обеспечение безопасности критической информационной инфраструктуры становится приоритетной государственной задачей. Устойчивое функционирование критической информационной инфраструктуры оказывает значительное влияние на социально-экономическое развитие России в условиях цифровой экономики, в том числе на безопасность бизнеса.

---

[266] См.: О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации № 683 от 31 декабря 2015 г. // СЗ РФ. 2016. № 1 (ч. II). Ст. 212.

[267] См.: В Пакистане введена смертная казнь за кибертерроризм // Информационный портал по безопасности SecurityLab.ru. URL: http://www.securitylab.ru/news/362634.php (дата обращения: 23.05.2019).

Злоумышленники постоянно совершенствуют технологии компьютерных атак на объекты критической информационной инфраструктуры. Ярким примером являются действия вредоносных компьютерных программ-вымогателей *WannaCry* и *Petya/Petrwrap/NotPetya/exPetr,* которые использовали для компьютерной атаки уязвимости в программном обеспечении пользователей[268]. Так, согласно данным аналитического отчета одного из лидеров европейского рынка систем анализа защищенности и соответствия стандартам – компании *Positive Technologies*, в первом квартале 2019 г. злоумышленники совершили около 58 % компьютерных атак на различные объекты информационной инфраструктуры[269].

Проблема безопасности критической информационной инфраструктуры уже давно интересует многих ученых. Несмотря на малое количество научных трудов по рассматриваемой теме, сложилась достаточно обширная методологическая база. При всем этом в анализе проблемы безопасности критической информационной инфраструктуры Российской Федерации остается немало нерешенных задач.

Изучение генезиса заявленного вопроса требует, прежде всего, уяснения понятия «безопасность».

По смыслу термин «безопасность» (от лат. *securitas*; англ. *safety, security*; фр. *securite*) означает отсутствие опасности, т. е. состояние, при котором опасность не угрожает.

В широком смысле слова термином «безопасность» обозначается ситуация, при которой вероятность причинения объекту защиты вреда и его возможные размеры, по мнению оценивающего

---

[268] Барташевич С. А. Информационная безопасность – залог успеха бизнеса // Information Security / Информационная безопасность. 2017. № 4. С. 19.

[269] Аналитический отчет «Актуальные киберугрозы. I квартал 2019 года» // Аналитический центр Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1–2019/#id5 (дата обращения: 23.05.2019).

ситуацию субъекта, меньше некоторого субъективно установленного им же предела[270].

Следовательно, в общем виде безопасность означает состояние защищенности личности, общества, государства от внутренних и внешних угроз или опасностей.

Понимание этого составляет основу дефиниции национальной безопасности Российской Федерации, закрепленной в Стратегии[271]. В свою очередь, национальная безопасность Российской Федерации существенным образом зависит от обеспечения информационной безопасности[272].

Наряду с этим информационная безопасность предполагает защищенность жизненно важных интересов личности, общества и государства непосредственно в информационной сфере[273].

Законодатель определяет безопасность критической информационной инфраструктуры Российской Федерации как состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак[274].

---

[270] Атаманов Г. А. Методология безопасности // Фонд содействия научным исследованиям проблем безопасности «НАУКА-XXI». URL: http://naukaxxi.ru/materials/302/ (дата обращения: 23.05.2019).

[271] См.: О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации № 683 от 31 декабря 2015 г. // СЗ РФ. 2016. № 1 (часть II). Ст. 212.

[272] Терещенко Л. К., Тиунов О. И. Информационная безопасность органов исполнительной власти на современном этапе // Журнал российского права. 2015. № 8. С. 107.

[273] Хисамова З. И. Понятие и сущность преступлений, посягающих на информационную безопасность в сфере экономики // Общество и право. 2015. № 1 (51). С. 157.

[274] См.: О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // СЗ РФ. 2017. № 31 (часть I). Ст. 4736.

Очевидно, что понятие «безопасность критической информационной инфраструктуры» является видовым по отношению к понятию «информационная безопасность», которая, в свою очередь, значится одним из видов безопасности и входит в понятие «национальная безопасность».

Таким образом, обеспечение безопасности критической информационной инфраструктуры должно основываться на принципах и методологии обеспечения национальной безопасности.

Закон о безопасности критической информационной инфраструктуры предписывает его субъектам обеспечить безопасность своих информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления.

Напомним, что в ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[275] отражены понятия информационной системы и информационно-телекоммуникационной сети. Понятие автоматизированной системы управления нашло свое отражение в ст. 2 «Основные понятия, используемые в настоящем Федеральном законе» Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[276]. Данное понятие носит в основном технологический характер и довольно широко используется в обиходе представителей технических специальностей.

В широком смысле слова автоматизированная система управления в какой-то степени состоит из информационной системы

[275] См.: Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 г. // СЗ РФ. 2006. № 31 (часть I). Ст. 3448.

[276] См.: О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // СЗ РФ. 2017. № 31 (часть I). Ст. 4736.

и информационно-телекоммуникационной сети, являющихся базовыми элементами критической информационной инфраструктуры, хотя и имеет свою особую технологическую основу, способную выделить ее в самостоятельный объект критической информационной инфраструктуры.

Видится, что наиболее тяжелым последствием компьютерных инцидентов является нарушение технологического процесса на предприятии. Это, в свою очередь, может, например, привести к повреждению выпускаемого продукта или снижению качества обслуживания клиентов, а также снижению объемов или временной остановке производства. Более того, возникает высокий риск техногенных аварий и экологических катастроф. Кроме того, подобные инциденты могут повлечь за собой снижение стоимости акций компании, репутационный ущерб, штрафные санкции, что также в конечном итоге может являться целью компьютерной атаки[277]. Поэтому мы считаем, что субъектам критической информационной инфраструктуры необходимо выстраивать слаженную систему своей информационной безопасности, а уже в рамках системы выполнять требования к обеспечению защиты информации. На наш взгляд, такие требования определены в соответствующих актах[278].

К субъектам критической информационной инфраструктуры отнесены государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предпри-

[277] Сердюк В. А. Некоторые аспекты защиты АСУ ТП // Information Security / Информационная безопасность. 2017. № 6. С. 12.

[278] См.: Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: Приказ Федеральной службы по техническому и экспортному контролю № 31 от 14 марта 2014 г. // Российская газета. 2014. № 175.

ниматели, 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 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[279].

При этом указанные субъекты критической информационной инфраструктуры *должны осуществлять свою деятельность только в некоторых социально-экономических сферах деятельности*[280].

По нашему мнению, помимо указанных сфер деятельности возможны и иные виды экономической деятельности, например, жилищно-коммунальное хозяйство, строительство, сельское хозяйство, пищевая промышленность и т. д. Однако указанные виды к субъектам критической информационной инфраструктуры *почему-то не отнесены, хотя в отношении их* информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления *также могут быть совершены компьютерные атаки*[281].

Предполагается, что, например, в результате компьютерных атак на сервисы для расчета и оплаты коммунальных услуг, мониторинга деятельности управляющих и ресурсоснабжающих организаций, состояния объектов государственного учета жилищного фонда может

---

[279] См.: О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // СЗ РФ. 2017. № 31 (часть I). Ст. 4736.

[280] Там же.

[281] Бегишев И. Р. Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 29.

быть нарушено функционирование государственной информационной системы жилищно-коммунального хозяйства[282], одной из важнейших социально значимых информационных систем государства.

В этой связи отметим, что, как представляется, законодателю еще предстоит отнести часть субъектов экономической деятельности, не нашедших отражения в действующем законодательстве, к субъектам критической информационной инфраструктуры.

По нашему мнению, для успешного решения этого вопроса необходимо использовать данные Общероссийского классификатора видов экономической деятельности (ОКВЭД 2)[283]. Именно по его данным следует соотносить вид экономической деятельности с предполагаемым субъектом критической информационной инфраструктуры.

Для более эффективного противодействия компьютерным атакам и обеспечения устойчивого функционирования объектов критической информационной инфраструктуры в условиях возникновения компьютерных инцидентов[284] в стране появи-

---

[282] О вводе в эксплуатацию государственной информационной системы жилищно-коммунального хозяйства: Приказ Министерства связи и массовых коммуникаций Российской Федерации № 264 от 14 июня 2016 г. // Министерство связи и массовых коммуникаций Российской Федерации: офиц. сайт. URL: http://minsvyaz.ru/ru/documents/5069/ (дата обращения: 15.05.2017).

[283] См.: О принятии и введении в действие Общероссийского классификатора видов экономической деятельности (ОКВЭД2) ОК 029–2014 (КДЕС Ред. 2) и Общероссийского классификатора продукции по видам экономической деятельности (ОКПД2) ОК 034–2014 (КПЕС 2008): Приказ Федерального агентства по техническому регулированию и метрологии № 14-ст от 31 января 2014 г. // Бухгалтерское приложение к газете «Экономика и жизнь». 2014. № 21.

[284] *Компьютерный инцидент* – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для органи-зации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

лась ГосСОПКА[285], полномочия по созданию которой возложены на органы безопасности[286] и органы государственной охраны[287]. На наш взгляд, подобная консолидация сил и средств указанных специальных служб позволит оперативно выявлять компьютерные атаки, пресекать их и снижать действие поражающих факторов при компьютерных инцидентах.

Заявлено, что главной задачей ГосСОПКА является осуществление государственного контроля за безопасностью критической информационной инфраструктуры Российской Федерации и степени их защищенности от компьютерных атак.

Однако следует отметить, что безопасность критической информационной инфраструктуры зависит не только от степени государственного контроля в этой сфере, но и от выполнения субъектами критической информационной инфраструктуры (бизнес-сообществом) конкретных требований по созданию систем безопасности и обеспечению их функционирования. Перечень таких требований определен соответствующим приказом ФСТЭК России[288].

---

[285] *ГосСОПКА* – государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

[286] См.: О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента Российской Федерации № 31с от 15 января 2013 г. // СЗ РФ. 2013. № 3. Ст. 178.

[287] См.: О внесении изменений в Положение о Федеральной службе охраны Российской Федерации, утвержденное Указом Президента Российской Федерации от 7 августа 2004 г. № 1013: Указ Президента Российской Федерации № 89 от 27 февраля 2018 г. // СЗ РФ. 2018. № 10. Ст. 1477.

[288] См.: Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: Приказ Федеральной службы по техническому и экспортному контролю № 235 от 21 декабря 2017 г. // Официальный интернет-портал правовой информации, 22 февраля 2018 г. URL: www.pravo.gov.ru

Повышение защищенности критической информационной инфраструктуры невозможно без должной оценки ее текущего состояния, всех рисков и угроз. На наш взгляд, объем финансовых расходов бизнес-сообщества на обеспечение информационной безопасности своей критической информационной инфраструктуры должен быть основан исключительно на вышеуказанной оценке. Это важнейший вопрос самосохранения бизнеса.

Механизмы классификации и категорирования объектов критической информационной инфраструктуры на сегодняшний день являются наиболее актуальными для субъектов, поскольку от них напрямую зависят финансовые затраты на обеспечение безопасности.

По нашему мнению, все объекты критической информационной инфраструктуры следует классифицировать на значимые и незначимые, поскольку только к значимым объектам можно предъявить специальные требования информационной безопасности. Именно по таким видам целесообразно классифицировать объекты критической информационной инфраструктуры[289].

К значимым объектам критической информационной инфраструктуры законодатель относит объекты, которые наделены категорией значимости[290] и включены в соответствующий реестр[291].

В свою очередь, в соответствии с ч. 3 ст. 7 «Категорирование объектов критической информационной инфраструктуры» Федерального закона «О безопасности критической информационной инфраструк-

---

[289] Бегишев И. Р. Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 30.

[290] См.: О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // СЗ РФ. 2017. № 31 (часть I). Ст. 4736.

[291] См.: Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ Федеральной службы по техническому и экспортному контролю № 227 от 6 декабря 2017 г. // Официальный интернет-портал правовой информации, 9 февраля 2018 г. URL: www.pravo.gov.ru

туры Российской Федерации» в отношении всех значимых объектов критической информационной инфраструктуры устанавливаются три категории значимости – 1, 2 и 3[292]. Такое деление должно быть поддержано субъектами критической информационной инфраструктуры, тем более что от выбранных значений показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации будет зависеть применение организационных и технических мер, обеспечивающих нейтрализацию (блокирование) угроз безопасности информации, последствиями которых может быть прекращение или нарушение функционирования объекта.

Постановлением Правительства Российской Федерации[293] установлено, что категорирование будет проводиться специально созданной комиссией субъекта на основании критериев значимости объектов критической информационной инфраструктуры. К таким показателям отнесены социально-экономическая и общественно-политическая значимость объекта критической информационной инфраструктуры.

Категорированию подлежат объекты критической информационной инфраструктуры, которые обеспечивают производственные, управленческие, технологические и иные процессы. Принципиально важно, чтобы все объекты критической информационной инфраструктуры принадлежали субъектам на законном основании. Иначе отнести их к значимым объектам невозможно.

Стоит указать, что субъекты критической информационной инфраструктуры обязаны:

---

[292] См.: О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // СЗ РФ. 2017. № 31 (часть I). Ст. 4736.

[293] См.: Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства Российской Федерации № 127 от 8 февраля 2018 г. // СЗ РФ. 2018. № 8. Ст. 1204.

1) разработать и утвердить перечень объектов критической информационной инфраструктуры, подлежащих категорированию;

2) согласовать с территориальным подразделением ФСТЭК России утвержденный перечень объектов критической информационной инфраструктуры;

3) согласовать с территориальным подразделением ФСТЭК России сроки проведения категорирования объектов;

4) провести мероприятия по категорированию объектов;

5) составить акт категорирования и направить его в территориальное подразделение ФСТЭК России.

Как нам представляется, мероприятия по категорированию объектов критической информационной инфраструктуры могут проводиться собственными силами субъектов, либо с привлечением сторонней организации, имеющей соответствующую лицензию ФСТЭК России по технической защите конфиденциальной информации.

Согласование со ФСТЭК России перечня объектов критической информационной инфраструктуры и сроков проведения их категорирования, направление акта категорирования являются обязательными для всех субъектов критической информационной инфраструктуры.

Наиболее значимый вклад в цифровую трансформацию российской экономики вносит реализация национальной программы «Цифровая экономика Российской Федерации», принятой в соответствии с Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[294] и утвержденной президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам (протокол

[294] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента Российской Федерации № 204 от 7 мая 2018 г. // СЗ РФ. 2018. № 20. Ст. 2817.

от 24 декабря 2018 г. № 16). Она включает шесть приоритетных направлений:

– нормативное регулирование цифровой среды (создание гибкой системы правового регулирования, обеспечивающей цифровую трансформацию отраслей экономики, социальной сферы и управления);

– информационная инфраструктура (создание глобальной конкурентоспособной инфраструктуры передачи, обработки и хранения данных, а также цифровых продуктов для граждан, бизнеса и власти);

– кадры для цифровой экономики (создание условий для пополнения рынка труда квалифицированными и конкурентоспособными кадрами в сфере цифровой экономики через трансформацию всех уровней системы образования, внедрения программ переобучения в компаниях и ведомствах);

– информационная безопасность (создание безопасной и устойчивой информационной инфраструктуры для граждан, представителей бизнеса и государства в цифровом пространстве);

– цифровые технологии (создание комплексной системы поддержки исследований, проектов по разработке, внедрению цифровых технологий и платформенных решений);

– цифровое государственное управление (переход к управлению данными государства на основе цифровых технологий, разработка комплексных суперсервисов для получения гражданами и бизнесом государственных услуг в один клик)[295].

Особое внимание в российской национальной программе уделено вопросам безопасности критической информационной инфраструктуры и внедрения цифровых технологий, в частности новых интеллектуальных технологий, поскольку в настоящее время началось формирование правовых основ применения искусственного интеллек-

[295] Там же.

та, что требует принятия действий и решений по предупреждению возможных негативных проявлений его использования и государственному реагированию на них[296]. Показано, что в процессе применения искусственного интеллекта возможны четыре ситуации, требующие уголовно-правового регулирования. Подчеркивается необходимость четкого, строгого и эффективного определения этических рамок при разработке, проектировании, производстве, использовании и модификации искусственного интеллекта[297]. Установлено, что в настоящее время не существует какого-либо единого международного нормативного акта, определяющего общую концепцию ответственности при совершении деяний, связанных с искусственным интеллектом[298].

Цифровая экономика является одним из главных двигателей роста и развития мировой экономики, открывающей безграничные возможности для бизнеса и государственного сектора. Информационные и телекоммуникационные технологии оказывают существенное влияние на развитие традиционных отраслей экономики. Внедрение цифровых технологий в глобальные производственные процессы в различных отраслях оказывает повсеместное влияние на характер производства[299].

Информационные и телекоммуникационные технологии оказывают существенное влияние на развитие традиционных отрас-

---

[296] Бегишев И. Р., Хисамова З. И. Криминологические риски применения искусственного интеллекта // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 767.

[297] Хисамова З. И., Бегишев И. Р. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты // Всероссийский криминологический журнал. 2019. Т. 13, № 4. С. 564.

[298] Денисов Н. Л. Концептуальные основы формирования международного стандарта при установлении уголовной ответственности за деяния, связанные с искусственным интеллектом // Международное уголовное право и международная юстиция. 2019. № 4. С. 18.

[299] Хисамова З. И. Международный опыт уголовно-правового противодействия преступлениям в сфере цифровой экономики. Краснодар: Изд-во Краснодар. ун-та МВД России, 2018. С. 5.

лей экономики. Внедрение цифровых технологий в глобальные производственные процессы в различных отраслях оказывает повсеместное влияние на характер производства[300].

При изучении общественных отношений, складывающихся по поводу уголовно-правовой регламентации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации и некоторых зарубежных стран[301], уста-

[300] Хисамова З. И. Законодательная регламентация уголовной ответственности за преступления, совершаемые в сфере цифровой экономики, в странах Юго-Восточной Азии // Общественная безопасность, законность и правопорядок в III тысячелетии. 2018. № 4–1. С. 366.

[301] См.: Wiater P. On the notion of "partnership" in critical infrastructure protection // European Journal of Risk Regulation. 2015. № 6 (2). Pp. 255–262; Hathaway O. A., Crootof R., Levitz P., Nix H. The Law of Cyber-Attack // California Law Review. 2012. № 100. Pp. 817–886; Shackelford S. J., Sulmey-er M., Craig Deckard A. N., Buchanan B., Micic B. From Russia with Love: Understanding the Rus-sian Cyber Threat to U.S. Critical Infrastructure and What to Do about It // Nebraska Law Review. 2017. № 96. Pp. 320–338; Albrecht D. Chinese Cybersecurity Law Compared to EUNIS-Directive and German IT-Security Act. When cybersecurity not only protects interests of the masses but ultimately also safeguards national sovereignty // Recherchieren unter juris (Das Rechtsportal). 2018. Pp. 1–5; Orji U. J. Towards the Regional Harmonization of E-Commerce Regulation in Africa A Comparative Anal-ysis of the African Union's E-Commerce Regime // Recherchieren unter juris (Das Rechtsportal). 2018. Pp. 12–22; Bovis C. H. Risk in public-private partnerships and critical infrastructure // European Journal of Risk Regulation. 2015. № 6 (2). Pp. 200–207; Brem S. Critical Infrastructure Protection from a Na-tional Perspective // European Journal of Risk Regulation. 2015. № 6 (2). Pp. 191–199; August T., August R., Shin H. Designing user incentives for cybersecurity // Communications of the ACM. 2014. № 57 (11). Pp. 43–46; Carr M. Public–private partnerships in national cyber-security strategies // Interna-tional Affairs. 2016. № 92 (1). Pp. 43–62; Dunn-Cavelty M., Suter M. Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection // International Jour-nal of Critical Infrastructure Protection. 2009. № 2 (4). Pp. 179–187; Min K.-S., Chai S.-W., Han M. An international comparative study on cyber security strategy // International Journal of Security and Its Applications. 2015. № 9 (2). Pp. 13–20; Walker C., Conway M. Online terrorism and online laws // Dy-namics of Asymmetric Conflict. 2015. № 8 (2). Pp. 156–175; Cohen-Almagor R. Internet architecture, freedom of expression and social responsibility: Critical realism and proposals for a better future // Innovation: The European Journal of Social Science Research. 2015. № 28 (2). Pp. 147–166.

новлено, что нормы зарубежного и российского законодательства, предусматривающие ответственность за посягательства на объекты критической информационной инфраструктуры, имеют в основном бланкетный характер.

Редакция ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ представляет собой структуру, являющуюся своего рода надстройкой над тремя преступлениями в сфере компьютерной информации:

– ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ;

– ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ;

– ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ.

По смыслу ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ по ней квалифицируются три перечисленных деяния, если они направлены против объектов критической информационной инфраструктуры. Таким образом, анализируемая уголовно-правовая норма в определенной мере конкурирует сразу с тремя статьями УК РФ (ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей») и является по некоторым критериям специальной по отношению к ним. В некотором смысле конструирование ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ противоречит сложившимся отечественным традициям криминализации и использования приемов

юридической техники при описании уголовно-правовых норм. Следуя им, установление более строгой уголовной ответственности за посягательства на объекты критической информационной инфраструктуры предпочтительнее было бы реализовать путем выделения соответствующих квалифицирующих и особо квалифицирующих признаков в ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ[302]. Мы солидарны с приведенным мнением ученых.

Полагаем, что уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации требует изменения.

Приведенный анализ показывает, что мировое цифровое пространство является целью хорошо организованных компьютерных атак. Методы и средства, используемые для их подготовки, постоянно совершенствуются. Такие компьютерные атаки могут быть направлены против различных объектов критической информационной инфраструктуры не только своего, но и зарубежных государств. Эффективное противодействие компьютерным атакам возможно только в рамках совместных усилий всех заинтересованных стран, прежде всего национальных уполномоченных органов в области обнаружения и предупреждения компьютерных атак, и унификации международного законодательства в сфере обеспечения безопасности критической информационной инфраструктуры.

---

[302] 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. № 2. С. 52.

Масштабный захват информационного пространства представителями различных криминальных кругов, лавинообразное распространение запрещенных контентов и активное паразитирование на социальных болезнях общества требуют от уголовной политики более внимательного и своевременного реагирования на подобные тенденции[303].

Одним из направлений в данный момент является законодательное регулирование информационного пространства, однако в одной отдельно взятой стране вряд ли это возможно. Необходимо законодательное регулирование только в рамках международного права. Тем более что тенденция к расширению международного сотрудничества в борьбе с преступностью в сфере высоких технологий отмечается в деятельности многих международных организаций и требует согласованного подхода государств к выработке норм, направленных на борьбу с ней[304]. В этой же связи Т. М. Лопатина указывала на важность принятия стратегии международного сотрудничества в сфере противодействия компьютерной преступности и предлагала приоритетные направления ее реализации[305].

Учитывая все вышесказанное, мы предлагаем разработать и внедрить:

– ФГОС ВО по направлению «Безопасность критической информационной инфраструктуры»;

---

[303] Козаев Н. Ш. Изменения в уголовной политике в связи с проблемами обеспечения безопасности интернет-пространства // Вестник Санкт-Петербургского университета МВД России. 2015. № 1 (65). С. 50.

[304] Шутова А. А. Техника имплементации норм международного права за информационные преступления в законодательство Российской Федерации в контексте интеграции мировых культур // Юридическая техника. 2016. № 10. С. 647.

[305] См.: Лопатина Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. … д-ра юрид. наук. М., 2006. 418 с.; Она же. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дис. … д-ра юрид. наук. М., 2006. 60 с.

– курсы переподготовки и повышения квалификации по направлению «Безопасность критической информационной инфраструктуры»;

– механизм повышения квалификации должностных лиц субъектов критической информационной инфраструктуры по различным вопросам обеспечения ее безопасности;

– механизм страхового обеспечения безопасности критической информационной инфраструктуры;

– механизм организации всероссийских, региональных и отраслевых киберучений на объектах критической информационной инфраструктуры Российской Федерации.

Таким образом, можно констатировать, что безопасность критической информационной инфраструктуры напрямую зависит от правильности принятия решений в деле противодействия компьютерным атакам, быстроты и эффективности действий их субъектов.

В заключение параграфа хотелось бы отметить, что, несмотря на принимаемые во всем мире меры безопасности, угроза кибертерроризма остается. Поэтому успешное решение этой проблемы возможно лишь совместными усилиями всех стран с использованием при этом принципов планомерности и системного подхода[306].

Подводя итоги второй главы исследования, сформулируем основные его выводы:

1. Поскольку общественная опасность неправомерного доступа к цифровой информации близка по своей сути и общественной опасности перехвату цифровой информации в пространстве и в связи с отсутствием в УК РФ нормы, предусматривающей ответственность за перехват цифровой информации, предлагается включить упоми-

[306] Рожков С. Ю. Кибертерроризм – угроза обществу // Материалы XI региональной научно-технической конференции «Вузовская наука – Северо-Кавказскому региону». Т. 1. Естественные и точные науки. Технические и прикладные науки. Ставрополь: СевКавГТУ, 2007. С. 201.

нание о данном деянии в наименование ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ и в диспозицию ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, изложив ее в следующей авторской редакции:

> *«Статья 272. Неправомерный доступ к охраняемой законом цифровой информации или ее перехват*
> *1. Неправомерный доступ к охраняемой законом цифровой информации, а равно незаконный ее перехват, если это деяние повлекло уничтожение, блокирование, модификацию, копирование цифровой информации, ознакомление с ней либо нарушение работы информационно-телекоммуникационных устройств, их систем и сетей,–*
> *наказывается…»* (далее по тексту УК РФ).

В примечании 3 к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ предлагаем дать определение понятия «перехват цифровой информации» в следующей редакции:

> *«Под перехватом цифровой информации понимается процесс неправомерного ее получения в пространстве».*

Следует отметить, что тезис об установлении уголовной ответственности за незаконный перехват охраняемой законом цифровой информации поддерживают более 64 % респондентов, принявших участие в экспертном опросе по проблемам уголовно-правового противодействия преступлениям в сфере обращения цифровой информации[307] (см. Приложения 1–3).

[307] Бегишев И. Р. Преступления в сфере обращения цифровой информации. Результаты научного исследования // Information Security / Информационная безопасность. 2012. № 6. С. 9.

2. Ввиду уточнения термина, указывающего на объекты обращения цифровой информации, обосновано предложение об изложении наименования ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ и диспозиции ч. 1 ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ в следующей авторской редакции:

> *«Статья 274. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей*
> *1. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом цифровой информации, причинившее крупный ущерб,–*
> *наказывается…»* (далее по тексту УК РФ).

3. Поскольку деяния, предусмотренные ст. 272, 273, 274, 274.1 УК РФ, представляют собой единую систему преступлений, посягающих на цифровую информацию, предлагается гл. 28 УК РФ назвать «Преступления в сфере обращения цифровой информации», а ст. 272, 273 и 274 УК РФ озаглавить как «Неправомерный доступ к цифровой информации или ее перехват», «Создание, использование и распространение вредоносных цифровых программ» и «Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей» соответственно.

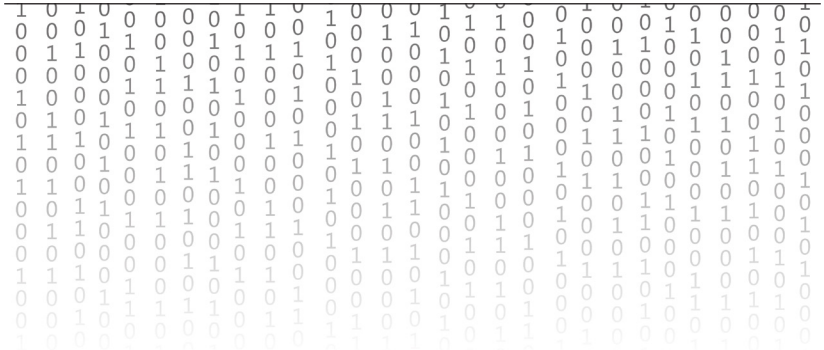
4. Раскрыты содержание и сущность понятия «безопасность критической информационной инфраструктуры». Обосновано,

что обеспечение безопасности критической информационной инфраструктуры должно строиться на принципах и методологии обеспечения национальной безопасности.

Выработаны предложения по отнесению части субъектов экономической деятельности к субъектам критической информационной инфраструктуры, предложены некоторые дополнительные механизмы повышения защищенности критической информационной инфраструктуры.

Доказано, что уголовно-правовая норма об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации требует совершенствования, и предложены его направления.

5. Предложено создание *Федеральной службы информационной безопасности Российской Федерации* – единого специального федерального органа исполнительной власти в сфере расследования и предупреждения преступлений в цифровой сфере, включая уголовно-правовое обеспечение безопасности объектов критической информационной инфраструктуры, а также воздействие на информационные инфраструктуры противника.



ГЛАВА 3

ИНЫЕ ВИДЫ ПРЕСТУПЛЕНИЙ И ОПАСНЫХ ДЕЯНИЙ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ, НУЖДАЮЩИЕСЯ В КРИМИНАЛИЗАЦИИ

§ 3.1. Мошенничество в сфере компьютерной информации

Игнорирование вопросов хищения чужого имущества в сфере обращения цифровой информации представляется недопустимым. Мир меняется, и мы меняемся вместе с ним. Нам, авторам монографии, как и огромному количеству сограждан, на служебную и личную электронную почту и телефон ежедневно приходят сообщения о выигрышах в конкурсах и лотереях, в которых мы даже не участвовали, огромных в денежном измерении призов. Либо об открывшемся за рубежом наследстве от ранее неизвестного лица, на которое мы можем претендовать. Вот только, чтобы приз или наследство получить, необходимо выполнить определенные условия… Потратить свои средства. Это каждодневное массовое мошенничество.

Многие ошибочно считают, что цифровые технологии надежно защищены от мошенничества в сфере компьютерной информации. Такой постулат неверен, чему есть большое количество практических примеров. Законодатель, убедившись в этом, включил ст. 159.6 «Мошенничество в сфере компьютерной информации»в УК РФ.

Она устанавливает уголовную ответственность за «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»[308].

Введение нормы, предусматривающей ответственность за мошенничество в сфере компьютерной информации, назрело давно, хотя не все ученые считают эту норму удачной и завершенной. Так, известный российский специалист в области уголовного права Н. А. Лопашенко, проанализировав новые составы мошенничеств, считает, что они выделены законодателем без каких-либо серьезных оснований[309]. В определенной мере с ней следует согласиться: множить сущности без необходимости нерационально.

Исходя из смысла, вложенного законодателем в содержание ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, нам представляется, что она содержит не специальный состав мошенничества, а самостоятельный вид хищения чужого имущества с присущими ей уникальными способами совершения преступления. Тем более что в диспозиции статьи не указаны такие основополагающие кримобразующие признаки собственно мошенничества, как совершение деяния путем обмана или злоупотребления доверием, как это сделано в ч. 1 ст. 159.6 УК РФ. Следует отметить, что в п. 1 постановления Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» разъяснено, что

---

[308] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 207-ФЗ от 29 ноября 2012 г. // СЗ РФ. 2012. № 49. Ст. 6752.

[309] Лопашенко Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы // Криминологический журнал Байкальского государственного университета экономики и права. 2015. № 3. С. 510.

способами хищения чужого имущества или приобретения права на чужое имущество при мошенничестве, ответственность за которое наступает в соответствии со статьями 158.1, 159, 159.1, 159.2, 159.3, 159.5 УК РФ, является обман или злоупотребление доверием, под воздействием которых владелец имущества или иное лицо передают имущество или право на него другому лицу либо не препятствуют изъятию этого имущества или приобретению права на него другим лицом[310]. Ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ в названном перечне отсутствует, что, как представляется, подтверждает нашу позицию о самостоятельности данного вида хищения.

Таким образом, представляется целесообразным изменить название данной статьи. На наш взгляд, более правильно было бы ввести в гл. 21 «Преступления против собственности» УК РФ новую норму, предусматривающую ответственность за совершение хищения с использованием компьютерной информации, как это предложила А. Ю. Чупрова[311].

Представляется, что общественную опасность мошенничества в сфере компьютерной информации определяет именно имущественный ущерб, причиняемый потерпевшему. Сами действия с компьютерной информацией, рассматриваемые вне связи с хищением чужого имущества или приобретением права на чужое имущество, не обязательно являются общественно опасными[312].

В контексте ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ приобретение права на чужое имущество

---

310 Постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» // Российская газета. 2017. № 280.

311 Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 134.

312 Харламов Д. И. Критерии криминализации новых видов мошенничества в УК РФ // Актуальные вопросы борьбы с преступлениями. 2016. № 1. С. 45.

является следствием мошеннических действий именно в компьютерно-информационной среде, когда происходит ввод информации, способствующей хищению, возникновению права на имущество, иные активы, удаления информации с целью совершения хищения, ее блокирования с целью недопущения доступа к информации, либо ее модификации, ведущей к искажению информации, вследствие чего возникают условия для совершения мошенничества[313].

Открытым является вопрос толкования терминов, использованных в рассматриваемом составе преступления.

Еще в 2008 г. С. С. Медведев пришел к выводу, что мошенничество в сфере высоких технологий гиперлатентно, поэтому оно общественно опасно в гораздо более высокой степени, чем «традиционное», следовательно, необходима его криминализация[314]. Он предлагал изменить ст. 159 «Мошенничество» УК РФ путем введения в нее нового квалифицирующего признака – «с использованием результата автоматизированной обработки данных»[315]. Данное предложение на момент его внесения считаем вполне обоснованным.

Интересную позицию занимал В. В. Хилюта. Он также до принятия указанного закона отмечал, что применение таких терминов, как «компьютерное мошенничество» и «компьютерная кража», является юридической фикцией[316]. По его мнению, к компьютерным преступлениям должны относиться только противоправные действия

---

313 Мнацаканян А. В. Информационная безопасность Российской Федерации: уголовно-правовые аспекты: дис. … канд. юрид. наук. М., 2015. С. 162.

314 Медведев С. С. Мошенничество в сфере высоких технологий: автореф. дис. … канд. юрид. наук. Краснодар, 2008. С. 14.

315 Там же. С. 7.

316 Хилюта В. В. Необходимость установления уголовной ответственности за хищения, совершаемые с использованием компьютерной техники // Криминологический журнал Байкальского государственного университета экономики и права. 2012. № 1. С. 30.

в изучаемой сфере, а УК РФ должен содержать норму, которая бы предусматривала ответственность за «хищение имущества путем модификации результатов автоматизированной обработки данных компьютерной системы». Предполагаемой нормой охватывались бы противоправные деяния, совершаемые с использованием средств компьютерной техники, сотовой связи, сети Интернет, поддельных банковских пластиковых карточек и т. д[317].

Введя в текст уголовного закона много новых терминов, законодатель, к сожалению, не определил их значения. Очевидно, что в правоприменительной деятельности по отношению к ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ возникают вопросы о том, какие действия следует относить к «вводу» и «удалению» компьютерной информации. Ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ оперирует понятием «уничтожение» компьютерной информации, но не упоминает ни о «вводе», ни об «удалении». В связи с этим закономерно возникает вопрос: существует ли какая-либо разница между «удалением» и «уничтожением» компьютерной информации?[318] Зачем в УК РФ заложена такая многозначность, в чем заключается замысел законодателя?

В.Г. Степанов-Егиянц справедливо отметил, что целесообразно дополнить ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ примечанием, в котором следует дать определение понятиям «ввод» и «уничтожение» компьютерной информации[319]. Подобный подход, выраженный в единообразном толковании указанных терминов, представляется нам корректным.

---

317 Там же.

318 Степанов-Егиянц В. Г. Совершение кражи и мошенничества с использованием компьютера или информационно-телекоммуникационных сетей // Риск: ресурсы, информация, снабжение, конкуренция. 2012. № 4. С. 394.

319 Там же. С. 394.

А. И. Халиуллин придерживается аналогичной позиции и отмечает, что в условиях отсутствия в нормативно-правовых актах логической границы между терминами «удаление» и «уничтожение» компьютерной информации их использование в качестве синонимов недопустимо. Приемлемым, по его мнению, является разграничение по признаку правомерности воздействия на информацию: «удаление» – предписанное или одобряемое, а «уничтожение» – противоправное и запрещенное законом воздействие на компьютерную информацию[320]. С данной позицией ученого следует согласиться.

Как справедливо отмечает А. Ю. Чупрова, уничтожение компьютерной информации, т. е. полная ее ликвидация, не является удалением и, соответственно, не может признаваться способом совершения деяния, предусмотренного ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ. В ситуации, когда хищение произошло путем уничтожения информации, необходима дополнительная квалификация содеянного по ст. 272–273 УК РФ[321].

Кроме того, некоторые ученые под уничтожением информации понимают ее состояние в виде, непригодном для использования[322].

Следует отметить, что содержание термина «уничтожение» применительно к информации определено законодателем не в уголовном, а в другом законе. Так, согласно ч. 8 ст. 3 «Основные понятия, используемые в настоящем Федеральном законе» Фе-

[320] Халиуллин А. И. Уголовно-правовой аспект неправомерного уничтожения компьютерной информации // Вестник Самарской гуманитарной академии. Серия: Право. 2013. № 2. С. 102.

[321] Чупрова А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 133.

[322] Белоус В. Г., Градицкая Н. С. Проблема квалификации хищений с использованием компьютерных технологий // Актуальные вопросы образования и науки. 2016. № 1–2. С. 52

дерального закона «О персональных данных»[323] «уничтожением персональных данных» являются «действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных»[324].

Спорно и содержание ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ. Способ совершения данного преступления как обязательный признак объективной стороны представляется возможным признаком преступлений в сфере компьютерной информации.

Наказуемость деяния также вызывает вопросы. Максимальная санкция по ч. 1 ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ ограничивается арестом на срок до четырех месяцев, а по ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ – лишением свободы до двух лет. Такая ситуация вызывает неоднозначное толкование и применение закона, так как неясно, каким образом квалифицировать содеянное: только по ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ или по совокупности преступлений. Судя по размеру наказаний за названные преступления, ч. 1 ст. 159.6 не может поглотить ч. 1 ст. 272 УК РФ, т.е. чаша весов, на наш взгляд, склоняется к совокупности.

А.В. Шеслер, например, считает, что если мошенничество, предусмотренное ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, совершается с использованием вредоносных компьютерных программ, то его следует квалифицировать по сово-

---

[323] О персональных данных: Федеральный закон № 152-ФЗ от 27 июля 2006 г. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3451.

[324] Халиуллин А. И. Уголовно-правовой аспект неправомерного уничтожения компьютерной информации // Вестник Самарской гуманитарной академии. Серия: Право. 2013. № 2. С. 102.

купности с ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ как создание, использование и распространение вредоносных компьютерных программ, совершаемые из корыстной заинтересованности[325].

Исходя из запрета применения аналогии закона к нормам УК РФ, а также в целях проведения более четкой границы между деянием, предусмотренным ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, и смежными составами преступлений, Н. Ш. Козаев вносит предложение о дополнении ч. 1 ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ после слов «информационно-телекоммуникационных сетей» словами «сопряженное с обманом пользователей компьютерной информации или информационно-телекоммуникационных сетей»[326]. Мы считаем целесообразным поддержать такой подход.

В п. 20 постановления Пленума Верховного Суда Российской Федерации № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» от 30 ноября 2017 г. разъясняется, что мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по ст. 272, 273 или 274.1 УК РФ. Таким образом,

---

[325] Шеслер А. В. Мошенничество: проблемы реализации законодательных новелл // Уголовное право. 2013. № 2. С. 70.

[326] См.: Козаев Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом: автореф. дис. … д-ра юрид. наук. Краснодар, 2016. С. 15; Он же. Современные проблемы уголовного права, обусловленные научно-техническим про-грессом. М.: Юрлитинформ, 2019. 480 с.; Он же. Противодействие злоупотреблениям современными технологиями: международно-правовые и уголовно-правовые аспекты. М.: Юрлитинформ, 2016. 192 с.

документ судебного толкования также рекомендует в соответствующих случаях обращаться к совокупности преступлений[327].

При этом в п. 21 данного постановления указано, что в тех случаях, когда хищение совершается путем использования учетных данных собственника или иного владельца имущества независимо от способа получения доступа к таким данным (тайно либо путем обмана воспользовался телефоном потерпевшего, подключенным к услуге «мобильный банк», авторизовался в системе интернет-платежей под известными ему данными другого лица и т.п.), такие действия подлежат квалификации как кража, если виновным не было оказано незаконного воздействия на программное обеспечение серверов, компьютеров или на сами информационно-телекоммуникационные сети. При этом изменение данных о состоянии банковского счета и (или) о движении денежных средств, происшедшее в результате использования виновным учетных данных потерпевшего, не может признаваться таким воздействием. А 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 ст. 159, а не 159.6 УК РФ[328]. Мы с этим толкованием согласны.

Однако квалификация по совокупности преступлений может иногда означать двойное, чрезмерное вменение. Совершая преступление, предусмотренное ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, лицо осознает, что изначально «транзитом»

[327] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда Российской Федерации № 48 от 30 ноября 2017 г. // Российская газета. 2017. № 280.

[328] Там же.

проходит через иное преступление – неправомерный доступ к компьютерной информации. Вследствие этого А. В. Кузнецов предлагает изменить диспозицию рассматриваемой статьи таким образом, чтобы способ совершения рассматриваемого вида мошенничества не ограничивался только неправомерным доступом к компьютерной информации (поскольку доступ может быть и правомерным), но и предусматривал иные возможности использования компьютерной техники, например, введение вредоносной программы и др.[329]

А. В. Кузнецов предлагает изложить диспозицию ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ в следующем виде: «...мошенничество в сфере компьютерной информации, то есть хищение чужого имущества или приобретение права на чужое имущество путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или направляемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации…»[330] Такой вывод тоже имеет право на существование и, по нашему мнению, является удачным.

Нам видится, что путем изменения не только компьютерной информации, но и вмешательством в технические средства ее обращения злоумышленник может похитить чужое имущество или приобрести право на чужое имущество.

В свою очередь возникает вопрос, что следует понимать под иным вмешательством в функционирование указанных средств и сетей. Обратимся в связи с этим к практике[331].

---

[329] Кузнецов А. В. Совершенствование правового регулирования уголовной ответственности за отдельные виды мошенничества // Научный вестник Омской академии МВД России. 2014. № 3. С. 30.

[330] Там же.

[331] Бегишев И. Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации // Вестник Казанского юридического института МВД России. 2016. № 3. С. 113.

Так, гр. А. в 2013 г. обнаружил документ с паспортными данными гр. Ф., после чего у него из корыстных побуждений возник преступный умысел на совершение хищения чужого имущества, а именно денежных средств гр. Ф. Гр. А., используя обнаруженные им паспортные данные гр. Ф., восстановив сим-карту, зарегистрированную на имя гр. Ф., путем ввода компьютерной информации в форме электрических сигналов – СМС-сообщений на номер 900, – перечислил, т.е. похитил, денежные средства на счет своей сим-карты, а затем со счета сим-карты гр. Ф. посредством услуги «Мобильный банк» ОАО «Сбербанк России» на лицевой счет принадлежащей ему банковской карты ОАО «Сбербанк России». Таким образом, гр. А. умышленно, из корыстных побуждений, путем иного вмешательства в функционирование информационно-телекоммуникационной сети похитил денежные средства, принадлежащие гр. Ф., причинив ему значительный материальный ущерб, незаконно изъяв похищенные денежные средства из владения потерпевшего, и распорядился ими впоследствии по своему усмотрению[332].

Сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, для удобства читателя приведены в Приложении 5.

Также открытым остается вопрос о таком способе совершения рассматриваемого преступления, как копирование компьютерной информации, который прямо в ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ не указан. Можно предположить, что это как раз разновидность иного вмешательства. Пу-

[332] См.: Приговор Андроповского районного суда Ставропольского края от 31 октября 2014 г. по уголовному делу № 1-97/2014. URL: https://rospravosudie.com/court-andropovskij-rajonnyj-sud-stavropolskij-kraj-s/act-461098820/ (дата обращения: 23.05.2019).

тем копирования компьютерной информации с последующим ее изменением и перенаправлением в нужном векторе также может быть совершено хищение. Данный вопрос остается открытым и не решенным законодателем.

Нам представляется, что мошенничество в сфере компьютерной информации может совершаться не только вышеописанными способами, но и с использованием вредоносных компьютерных программ. К такому классу программ можно отнести и мошенническое программное обеспечение по следующим основаниям.

Согласно ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ, под вредоносными компьютерными программами понимаются программы, заведомо предназначенные для несанкционированного уничтожения, копирования, модификации, блокирования компьютерной информации или нейтрализации средств ее защиты. В свою очередь, на основе анализа диспозиции ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ можно предположить, что мошенническое программное обеспечение (мошеннические программы) – это программы, заведомо позволяющие вводить, удалять, блокировать, модифицировать компьютерную информацию либо осуществлять иное вмешательство в функционирование указанных средств и сетей. Таким образом, мошеннические программы по способу деструктивного воздействия на компьютерную информацию, результату воздействия, наличию целей и мотивов являются аналогичными вредоносным цифровым программам.

На сегодняшний день таким мошенническим программным обеспечением выступают, например:

– программы-баннеры, всплывающие в окнах интернет-браузера;

– программы-блокираторы, перекрывающие доступ в информационно-телекоммуникационную сеть Интернет;

– программы-блокираторы, препятствующие возможностям операционной системы *Windows*, а также действиям с файлами;

– программы-шифровальщики, кодирующие файлы.

Общей особенностью этого вида мошеннических программ является то, что устранение их деструктивных действий обычно происходит в результате отправки потерпевшим на известный номер телефона платного СМС-сообщения. Иными словами, от него требуют выкуп как условие прекращения каких-либо ограничений.

Однако уже сегодня можно с уверенностью констатировать, что мошенничество в сфере компьютерной информации будет только наращивать обороты и все в больших размерах и многообразии появляться в электронной коммерции, на электронных площадках оплаты товаров и услуг, в секторе дистанционного банковского обслуживания и т. д. Цифровизация всего только нарастает, и это множит риски. Опасность широкого распространения угрозы цифрового мошенничества налицо.

Динамичное развитие электронных систем и коммуникаций и их повсеместное внедрение способствовало увеличению количества совершаемых в соответствующих сферах преступлений. При этом большая часть посягательств происходит в сфере дистанционного банковского обслуживания и электронной коммерции, что напрямую влияет на устойчивость экономики государства[333].

Безналичная система расчетов на основе использования банковских платежных карт продолжает активно внедряться в кредитно-финансовую сферу деятельности нашей страны, являясь при этом привлекательным объектом как для отдельных преступников, так и для организованных преступных групп. Расширение спектра предоставленных банками услуг в безналичной сфере расчетов

[333] Хисамова З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа // Государство и право. 2015. № 3. С. 128.

неизбежно приводит к изменениям в структуре экономической преступности[334].

Рассуждая о мошенничестве в сфере цифровой информации, нельзя не сказать о мошенническом программном обеспечении, позволяющем нарушать системы защиты цифровой информации. Сегодня зачастую такое программное обеспечение находится в свободном доступе в сети Интернет или же нелегально приобретается на соответствующих виртуальных площадках у их разработчиков. Таким образом, ограничение в создании, использовании и распространении такого программного обеспечения существенно затруднило бы злоумышленникам совершение подобного рода мошенничеств. Это также касается рассматриваемых программ и программных средств, используемых для нарушения систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей[335].

Поэтому предлагаем включить в «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»[336], сайты, содержащие или распространяющие вредоносные компьютерные программы, мошенническое программное обеспечение и программные средства, предназначенные для нарушения систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей.

---

334 Хисамова З. И. Кардерство в современной России // Вестник Краснодарского университета МВД России. 2012. № 3 (17). С. 97.

335 Бегишев И. Р. Новый взгляд на мошенничество в сфере компьютерной информации // Information Security / Информационная безопасность. 2016. № 1. С. 28.

336 Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 г. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

Такой механизм предупреждения мошенничества в сфере компьютерной информации, по нашему мнению, является наиболее эффективным. Провайдеры хостинга и операторы связи используют указанный единый реестр и успешно ограничивают доступ к таким ресурсам.

Следует отметить, что за создание, формирование и ведение указанного реестра отвечает Роскомнадзор[337]. Ведение реестра осуществляется в электронной форме в ежедневном круглосуточном режиме.

Необходимо сказать, что аналогичные схемы уже работают и успешно применяются на практике в отношении, например, материалов с порнографическими изображениями несовершеннолетних, информации о способах совершения самоубийства, информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами, и др.[338]

Многие современные антивирусные программы в своем составе имеют модули, позволяющие распознать и прекратить распространение мошеннического программного обеспечения. Однако некоторые пользователи информационно-телекоммуникационной сети Интернет не могут или не желают платить за антивирусное программное обеспечение и не устанавливают его на свои компьютеры, тем самым способствуя совершению в их отношении мошеннических действий.

В.Г. Степанов-Егиянц подчеркивает, что не является преступлением использование вредоносной программы для личных нужд,

---

[337] О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено»: Постановление Правительства Российской Федерации № 1101 от 26 октября 2012 г. // СЗ РФ. 2012. № 44. Ст. 6044.

[338] Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 г. // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448.

использование вредоносных программ организациями, осуществляющими разработку антивирусных программ[339]. Мы поддерживаем такую точку зрения, поскольку ущерб охраняемым уголовным законом объектам в таких случаях не причинен.

Представляется, что мошенничество в сфере компьютерной информации может совершаться не только с использованием вредоносных компьютерных программ, но и с нарушением систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей. В действующей редакции ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ об этом ничего не сказано, хотя данное деяние часто встречается на практике. Следует отметить, что данный массив преступлений тесно связан с незаконным производством, приобретением и (или) сбытом специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

Проблемы правового ограничения обращения и применения специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, подробно рассмотрены ранее[340]. К схожим выводам пришли Р. Б. Иванченко и А. Н. Малышев, считающие, что хищение или приобретение права на чужое имущество сопряжено с преодолением компьютерной защиты имущества (имущественных прав). При этом авторы отмечают, что в действующей редакции ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ о сопряженности хищения с преодолением компьютерной защиты имущества

---

[339] Степанов-Егиянц В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): дис. … д-ра юрид. наук. М., 2016. С. 386.

[340] Бегишев И. Р. Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект // Информация и безопасность. 2010. № 2. С. 255–258.

(имущественных прав) ничего не сказано[341]. Мы разделяем данную позицию.

Н. А. Лопашенко пришла к выводу, что мошенничество с использованием информационных технологий – это деяние, совершаемое с корыстной направленностью, связанное с внесением изменений в компьютерные данные либо распространением ложных сведений по компьютерным сетям[342]. Распространение ложных сведений по компьютерным сетям в контексте рассматриваемой статьи тоже имеет место.

Кроме того, передача может осуществляться любым способом, позволяющим воспринимать информацию[343]. Под распространением подразумевается в первую очередь передача какой-либо информации неопределенному кругу лиц[344] или ее предоставление в любой форме хотя бы одному лицу (устной, письменной, с использованием информационных технологий, СМИ или информационно-телекоммуникационных сетей)[345].

---

[341] Иванченко Р. Б., Малышев А. Н. Проблемы квалификации мошенничества в сфере компьютерной информации // Вестник Воронежского института МВД России. 2014. № 1. С. 196.

[342] Преступность, уголовная политика, уголовный закон: сб. науч. тр. / под ред. Н.А. Лопашенко; Саратовский Центр по исследованию проблем организованной преступности

[343] Шутова А. А. Распространение сведений как способ совершения информационных преступлений // Материалы Международной научно-практической конференции «Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований», г. Санкт-Петербург, 11 декабря 2015 г.: СПб.: Санкт-Петербургский университет МВД России, 2016. С. 255.

[344] Шутова А. А. Распространение сведений как способ совершения информационных преступлений // Материалы XIV Международной научно-практической конференции «Татищевские чтения: актуальные проблемы науки и практики», г. Тольятти, 20–21 апреля 2017 г.: в 4 т. / Мин-во образования и науки Самарской обл., Мэрия г. о. Тольятти Самарской обл., Волжский ун-т им. В. Н. Татищева. Тольятти: Волжский ун-т им. В. Н. Татищева, 2017. С. 289.

[345] Шутова А. А. Уголовно-правовая охрана деловой репутации юридических лиц // Вестник Российского университета кооперации. 2016. № 3 (25). С. 142.

Существуют и другие научные позиции. Так, Р. Б. Иванченко и А. Н. Малышев полагают необоснованной криминализацию деяний, предусмотренных ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ. Они считают, что с учетом специфики предмета, способа и средств совершения анализируемых преступлений в УК РФ следует предусмотреть статью «Хищение с использованием компьютерной информации», в которой предлагается установить ответственность за такое хищение, если при этом используется несанкционированное вмешательство в функционирование указанных средств и сетей[346]. Аналогичной точки зрения придерживается М. А. Ефремова, сделавшая вывод о том, что не совсем ясна цель, которую преследовал законодатель, включив ст. 159.6 «Мошенничество в сфере компьютерной информации»в УК РФ[347]. Нам видится, что норма, предусматривающая ответственность за мошенничество в сфере компьютерной информации, еще досконально не изучена и несовершенна.

Существует и противоположная точка зрения. Так, А. Ю. Филаненко в целях отграничения мошенничества от неправомерного доступа предлагает изменить ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ путем включения в ч. 1 указанной статьи после слов «компьютерной информации» слов «без целей хищения чужого имущества или приобретения права на чужое имущество»[348]. Такое мнение тоже имеет право на существование и, по сути, частично решает существующую проблему.

---

[346] См.: Иванченко Р. Б., Малышев А. Н. Указ. раб. С. 198.

[347] Ефремова М. А. Мошенничество с использованием электронной информации // Информационное право. 2013. № 4. С. 20.

[348] Филаненко А. Ю. Отграничения мошенничества в компьютерной информации от неправомерного доступа // Право и государство: теория и практика. 2013. № 1. С. 62.

В заключение параграфа сформулируем некоторые предложения, направленные на совершенствование нормы, предусматривающей ответственность за мошенничество в сфере компьютерной информации, и некоторые механизмы противодействия такому мошенничеству:

– поскольку деяние, предусмотренное ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, относится к преступлениям в сфере обращения цифровой информации и совершается с ее использованием, то указанную статью предлагается назвать «Мошенничество с использованием цифровой информации»;

– аргументировано, что мошенническое программное обеспечение относится к категории вредоносных цифровых программ. Уголовная ответственность за создание, использование и распространение мошеннического программного обеспечения (мошеннических программ) должна наступать по ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ;

– с целью дифференциации ответственности за мошенничество в сфере цифровой информации предлагается внести в ч. 2 ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ следующий квалифицирующий признак: после слов *«значительного ущерба гражданину»* указать *«или с нарушением системы защиты цифровой информации»*;

– поскольку информационно-телекоммуникационная сеть «Интернет» содержит интернет-ресурсы, размещающие информацию о вредоносных компьютерных программах и программных средствах, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей, предлагается в целях предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «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» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом:

> *«ж) вредоносных программ и программных средств, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей».*

§ 3.2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации

В ч. 2 ст. 23 Конституции Российской Федерации указано, что каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а ограничение этого права допускается только на основании судебного решения[349]. В связи с этим можно заключить, что тайна сообщений человека и гражданина подлежит повышенной защите.

Общественная опасность несанкционированного съема информации выражается в посягательстве на информацию, содержащую сведения конфиденциального характера. Все чаще преступники используют данную информацию для совершения преступлений,

[349] Конституция Российской Федерации (в редакции Закона Российской Федерации о поправке к Конституции Российской Федерации от 21 июля 2014 г. № 11-ФКЗ) // Российская газета. 1993. № 237; СЗ РФ. 2014. № 31. Ст. 4398.

связанных с фальсификацией телефонных разговоров и т. д., нарушая при этом тайну телефонных переговоров.

Уголовная ответственность за нарушение указанной тайны была подробно рассмотрена М. А. Ефремовой[350]. Во многих случаях нарушение названного вида тайны невозможно без использования специальных технических средств[351].

К таким специальным техническим средствам, в частности, относят устройства заводского и самостоятельного изготовления, технические средства, приборы, различные приспособления, с помощью которых снимается и расшифровывается информация с технических каналов связи: сверхплоские и миниатюрные радиопередатчики; приспособления для прослушивания телефонных разговоров; аппаратура перехвата информации с каналов мобильной связи и т. д.[352]

Изготовление электронных средств, электронных носителей информации, технических устройств, компьютерных программ представляет собой совокупность технологических процессов, направленных на создание вышеназванных устройств и программ[353].

Независимо от способа изготовления специальных технических средств законодатель определил, что незаконные производство, приобретение и (или) сбыт специальных технических средств,

---

[350] См.: Ефремова М. А. Уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений // Вестник Казанского юридического института МВД России. 2015. № 1. С. 56.

[351] См.: Бегишев И. Р. Проблемы уголовной ответственности за обращение со специальными техническими средствами, предназначенными для негласного получения информации // Следователь. 2010. № 5. С. 2.

[352] Специальные радиосистемы: сайт. Форум. URL: http://www.radioscanner.ru/forum/topic46225-8.html (дата обращения: 23.05.2019).

[353] Хисамова З. И. Неправомерный оборот средств платежей в контексте норм об ответственности за преступления, совершаемые в отношении информационно-коммуникационных технологий // Общество и право. 2015. № 4 (54). С. 142.

предназначенных для негласного получения информации,– уголовно наказуемое деяние.

Перечень специальных технических средств, используемых в процессе осуществления оперативно-розыскной деятельности, определен Правительством Российской Федерации[354].

В ст. 6 «Оперативно-розыскные мероприятия» Федерального закона «Об оперативно-розыскной деятельности» установлен запрет на использование специальных технических средств, предназначенных для негласного получения информации, не уполномоченными на то настоящим федеральным законом физическими и юридическими лицами[355]. То есть прослушивания переговоров телефонных, например, разрешены только субъектам оперативно-розыскной деятельности в установленном законом порядке.

Основания для проведения снятия информации с технических каналов связи и связанные с такой деятельностью проблемные вопросы соблюдения прав и свобод человека и гражданина были подробно рассмотрены А. И. Анапольской и В. Н. Влазневым[356].

---

[354] Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности: Постановление Правительства Российской Федерации № 770 от 1 июля 1996 г. // СЗ РФ. 1996. № 28. Ст. 3382.

[355] См.: Об оперативно-розыскной деятельности: Федеральный закон № 144-ФЗ от 12 августа 1995 г. // СЗ РФ. 1995. № 33. Ст. 3349.

[356] См.: Анапольская А. И., Влазнев В. Н. Снятие информации с технических каналов связи: условия гарантирования прав и свобод человека и гражданина // Вопросы современной науки и практики. Университет им. В. И. Вернадского. 2015. № 2. С. 96.

Разработка, производство, реализация и приобретение в целях продажи таких средств подлежат лицензированию в соответствии с законодательством Российской Федерации[357]. Лицензирование указанной деятельности осуществляется Федеральной службой безопасности Российской Федерации[358].

С. Д. Петроченков считает, что разработку указанных средств нужно выделять как самостоятельное действие и понимать под ней создание нового технического средства или конструктивное усовершенствование старого[359].

Перечень видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензиро-ванию, устанавливается Правительством Российской Федерации[360]. Так, к специальным техническим средствам для негласного прослушивания телефонных переговоров, в частности, относятся:

– системы проводной связи, предназначенные для негласного прослушивания телефонных переговоров;

---

[357] См.: Об оперативно-розыскной деятельности: Федеральный закон № 144-ФЗ от 12 августа 1995 г. // СЗ РФ. 1995. № 33. Ст. 3349.

[358] См.: Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации: Постановление Правительства Российской Федерации № 287 от 12 апреля 2012 г. // СЗ РФ. 2012. № 16. Ст. 1885.

[359] Петроченков С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации. М.: ЮНИТИ-ДАНА, 2017. 135 с.

[360] Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию: Постановление Правительства Российской Федерации № 214 от 10 марта 2000 г. // СЗ РФ. 2000. № 12. Ст. 1292.

– радиоаппаратура, предназначенная для негласного прослушивания телефонных переговоров;

– специальные технические средства для негласного перехвата и регистрации информации с технических каналов связи[361].

Согласно этому документу, специальные технические средства могут быть как закамуфлированными под бытовые предметы, так и незакамуфлированными, если это не указано специально[362].

Однако однозначно решить, относится ли то или иное техническое средство к специальным техническим средствам, может только суд, исходя из заключения эксперта и анализа обстоятельств использования изъятого технического средства.

При отнесении технических устройств к специальным техническим средствам, предназначенным для негласного получения информации, суд, полагая, что решение этого вопроса требует специальных познаний, ссылается, как правило, на заключение эксперта или показания специалиста, которые, в свою очередь, руководствуются Постановлением Правительства Российской Федерации от 10 марта 2000 г. № 214, указывая, прежде всего, на признак камуфлированности и используя не специальные, а юридические познания[363].

С. Д. Петроченков справедливо отмечал в свое время, что ни в одном из нормативных правовых актов не раскрывается понятие специальных технических средств, что вызывает на практике массу спорных ситуаций при отнесении к ним тех или иных технических

---

[361] Там же.

[362] Петроченков С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации // Вестник Московского университета МВД России. 2012. № 6. С. 75.

[363] Петроченков С. Д. К вопросу о предмете преступления, предусмотренного ст. 138.1 Уголовного кодекса Российской Федерации // Труды Академии управления МВД России. 2016. № 3 (39). С. 25.

устройств[364]. Кроме того, он указывал, что норма рассматриваемой статьи носит бланкетный характер, что вызывает необходимость обращения к обширному законодательству, регулирующему оборот рассматриваемых средств. Указанное законодательство состоит из множества нормативных правовых актов самого различного уровня, начиная с международных документов и заканчивая ведомственными правовыми актами. По его мнению, все эти документы не только не составляют единую систему, но зачастую противоречат друг другу, содержат законодательные пробелы[365]. С данной позицией нельзя не согласиться.

С. Д. Ковалев и Е. В. Полуянова также высказывались, что в нормативной базе, регулирующей сферу правоотношений по применению специальных технических средств, имеются определенные пробелы, а некоторые из ныне действующих нормативных правовых актов не учитывают современный уровень развития технических средств[366]. С этим мнением мы также солидарны.

В п. 2 Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденного Постановлением Правительства Российской

---

[364] Петроченков С. Д. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации: законодательный подход и судебная практика // Пробелы в российском законодательстве. 2012. № 3. С. 155.

[365] См.: Петроченков С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации: дис. … канд. юрид. наук. М., 2013. С. 25.

[366] Ковалев С. Д., Полуянова Е. В. Формирование понятия «специальные технические средства»: исторический, научный и практический аспекты // Пенитенциарное право: юридическая теория и правоприменительная практика. 2016. № 3. С. 75.

Федерации от 16 апреля 2012 г. № 314 «Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)»[367], приводится определение данного устройства: «...специально изготовленное изделие, содержащее электронные компоненты, скрытно внедряемое (закладываемое или вносимое) в места возможного съема защищаемой акустической речевой, визуальной или обрабатываемой информации (в том числе в ограждения помещений, их конструкции, оборудование, предметы интерьера, а также в салоны транспортных средств, в технические средства и системы обработки информации)». Очевидно, что электронные устройства являются разновидностью технических средств, предназначенных для негласного получения информации. Поэтому граница между противоправным деянием и правомерным действием не определена вследствие отсутствия четкой дефиниции таких средств, их исчерпывающего перечня, признаков и критериев отграничения от технических средств, разрешенных к обороту[368]. Мы согласны с этой точкой зрения.

Большой научный и практический интерес вызывает вопрос отнесения технических средств, обладающих возможностью негласного получения информации, к категории специальных.

Отметим, что по смыслу правовой позиции Конституционного суда Российской Федерации, выраженной в постановлении от 31 марта 2011 г. № 3-П, в силу предписаний Конституции Российской Федерации технические средства (предметы, устройства),

---

[367] СЗ РФ. 2012. № 17. Ст. 1988.

[368] Радченко О. В., Габеев С. В. Проблемы квалификации незаконного оборота специальных технических средств, предназначенных для негласного получения информации // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2014. № 3. С. 29.

которые по своим техническим характеристикам, параметрам, свойствам или прямому функциональному предназначению рассчитаны лишь на бытовое использование массовым потребителем, не могут быть отнесены к специальным техническим средствам, предназначенным для негласного получения информации, если только им намеренно не приданы нужные качества и свойства, в том числе путем специальной технической доработки, программирования именно для неочевидного, скрытного их применения. Поскольку специальные технические средства, предназначенные для негласного получения информации, в силу присущих им свойств предоставляют эффективную возможность серьезно вторгаться в уязвимую для внешнего вмешательства сферу частной жизни, в личное пространство и личные интересы индивида без его согласия, неконтролируемое и не обусловленное конституционно признаваемыми целями их использование ведет к нарушению прав личности[369].

Проанализируем содержание термина «специальное техническое средство, предназначенное для негласного получения информации». Необходимо отметить, что перечень таких технических средств, утвержденный решением Коллегии Евразийской экономической комиссии от 21 апреля 2015 г. № 30 «О мерах нетарифного регулирования»[370], не дает возможности выделить характеризующие их признаки. Более того, действующие нормативные правовые акты не учитывают современный уровень их развития[371].

---

[369] См.: По делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С. В. Капорина, И. В. Коршуна и других: Постановление Конституционного Суда Российской Федерации № 3-П от 31 марта 2011 г. // СЗ РФ. 2011. № 15. Ст. 2191.

[370] Евразийский экономический союз: сайт // Правовой портал. 22 апреля 2015 г. URL: https://docs.eaeunion.org (дата обращения: 23.05.2019)

[371] Лопатина Т. М. Трансформация уголовного права и уголовного процесса в условиях развития цифровых технологий: на примере использования специальных технических средств, предназначенных для негласного получения информации // Библиотека криминалиста. Научный журнал. 2018. № 3 (38). С. 65.

В. Т. Батычко считает, что специальные технические средства – любые технические средства и приспособления, с помощью которых добывается информация о переписке, телефонных переговорах, почтовых, телеграфных и иных сообщениях граждан. К ним, например, относятся видео- и аудиозапись, кино- и фотосъемка и другие технические средства, не причиняющие вреда жизни и здоровью личности и окружающей среде[372]. Данная точка зрения представляется неточной.

Из самой формулировки специальных технических средств, предназначенных для негласного получения информации, вытекают три основных их нормативно определенных признака:

– это средство предназначено для негласного получения информации;

– это средство техническое;

– это средство специальное.

Термин «специальное», на наш взгляд, в рассматриваемом определении использовать нецелесообразно, так как оно неоправданно сужает круг предметов преступления и может трактоваться неоднозначно. Например, как специально созданное для негласного получения информации.

Так, возникает вопрос: подпадают ли под указанное определение понятия «специальное техническое средство» такие технические средства, используемые в повседневной жизни, как фото- и видеокамеры, магнитофоны, диктофоны и т. д.? А также относятся ли к ним иные средства, используемые для негласного получения информации, если использование названных предметов для указанной цели представляет общественную опасность?

Пункт 8 постановления Пленума Верховного Суда Российской Федерации от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституци-

[372] Батычко В. Т. Уголовное право. Общая и Особенная части. Курс лекций. Таганрог, 2006. С. 130.

онных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)» гласит, что по смыслу закона технические устройства (смартфоны, диктофоны, видеорегистраторы и т. п.) могут быть признаны специальными техническими средствами только при условии, если им преднамеренно путем технической доработки, программирования или иным способом приданы новые качества и свойства, позволяющие с их помощью негласно получать информацию. Там же говорится, что в случаях, когда для установления принадлежности технического устройства к числу средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, требуются специальные знания, суд должен располагать соответствующими заключениями специалиста или эксперта[373]. Таким образом, Пленум Верховного Суда Российской Федерации термин «специальный» толкует как приспособленный для негласного получения информации. В итоге «масло масляное» получается, поскольку о предназначенности для негласного получения информации говорится отдельно.

Федеральный закон от 2 августа 2019 г. № 308-ФЗ «О внесении изменения в статью 138.1 Уголовного кодекса Российской Федерации» дополнил указанную статью примечанием 1, согласно которому под специальными техническими средствами, предназначенными для негласного получения информации, в настоящем кодексе понимаются приборы, системы, комплексы, устройства, специальные инструменты для проникновения в помещения и (или) на другие объекты и программное обеспечение для электронных вычислительных машин и других электронных устройств для доступа

[373] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации): Постановление Пленума Верховного Суда Российской Федерации № 46 от 25 декабря 2018 г. // Российская газета. 2019. № 1.

к информации и (или) получения информации с технических средств ее хранения, обработки и (или) передачи, которым намеренно приданы свойства для обеспечения функции скрытого получения информации либо доступа к ней без ведома ее обладателя. А в соответствии с также вновь принятым примечанием 2 «к специальным техническим средствам, предназначенным для негласного получения информации, не относятся находящиеся в свободном обороте приборы, системы, комплексы, устройства, инструменты бытового назначения, обладающие функциями аудиозаписи, видеозаписи, фотофиксации и (или) геолокации, с открыто расположенными на них органами управления таким функционалом или элементами индикации, отображающими режимы их использования, или наличием на них маркировочных обозначений, указывающих на их функциональное назначение, и программное обеспечение с элементами индикации, отображающими режимы его использования и указывающими на его функциональное назначение, если им преднамеренно путем специальной технической доработки, программирования или иным способом не приданы новые свойства, позволяющие с их помощью получать и (или) накапливать информацию, составляющую личную, семейную, коммерческую или иную охраняемую законом тайну, без ведома ее обладателя»[374].

Получается, УК РФ основным признаком рассматриваемого предмета признал наличие функции скрытого получения информации либо доступа к ней без ведома ее обладателя. Эта позиция примыкает, на наш взгляд, к описанному выше подходу Пленума Верховного Суда РФ, просто сформулирована иными словами. Таким образом, фото- и видеокамеры, магнитофоны, диктофоны и т.п. могут быть признаны специальными техническими средствами, предназначенными для негласного получения информации, если

[374] См.: О внесении изменения в статью 138.1 Уголовного кодекса Российской Федерации: Федеральный закон № 308-ФЗ от 2 августа 2019 г. // СЗ РФ. 2019. № 31. Ст. 4467.

они закамуфлированы (скрыты) и их использование возможно без ведома соответствующего лица.

На наш взгляд, законодательное определение понятия специальных технических средств, предназначенных для негласного получения информации, является слишком запутанным и громоздким. Мы предлагаем под таким средством понимать программное либо аппаратное устройство, созданное или приспособленное для негласного перехвата, обработки и анализа информации.

Г. В. Семенов предлагал выделение ч. 3 ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ в качестве самостоятельного состава преступления, с включением в данную норму ответственности, в том числе за неправомерное использование специальных технических средств применительно к защищаемым законом видам информации[375]. Законодатель поступил несколько иначе – внес изменения в УК РФ, включив в него ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ[376].

Законодатель в свое время ввел и сейчас сохраняет уголовную ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации, в определенной степени базируясь на положениях Федерального закона от 29 апреля 2008 г. № 57-ФЗ [377]. В нем сказано о том, что

[375] Семенов Г. В. Расследование преступлений в сфере мобильных телекоммуникаций. М.: Юрлитинформ, 2006. С. 34.

[376] См.: О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 420-ФЗ от 7 декабря 2011 г. // СЗ РФ. 2011. № 50. Ст. 7362.

[377] См.: О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства: Федеральный закон № 57-ФЗ от 29 апреля 2008 г. // СЗ РФ. 2008. № 18. Ст. 1940.

разработка, производство, реализация и приобретение в целях продажи специальных технических средств, предназначенных для негласного получения информации, относятся к видам деятельности, имеющим стратегическое значение для обеспечения обороны страны и безопасности государства. Не вызывает сомнений тот факт, что бесконтрольный оборот специальных технических средств, предназначенных для негласного получения информации, создает благоприятную почву для шпионажа и утечки государственных секретов. Поэтому безопасность государства следует считать той основной целью, для достижения которой установлена уголовная ответственность, в том числе за незаконный оборот специальных технических средств, предназначенных для негласного получения информации[378].

В свете изложенного предлагаем вместо термина «специальные технические средства, предназначенные для негласного получения информации» использовать в УК РФ более точный и недвусмысленный термин «технические средства негласного получения информации».

Анализ материалов опубликованной судебной практики судов общей юрисдикции Российской Федерации, размещенных в открытом доступе на интернет-ресурсе «Судебные и нормативные акты РФ»[379], позволил сделать вывод, что к числу основных противоправных деяний, предусмотренных ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ, относится незаконное приобретение специальных технических средств, предназначенных для негласного получения информации в информационно-телекоммуникационной сети

[378] Новиков В. А. Дискуссионные аспекты определения границ видового объекта преступлений, предусмотренных главой 19 УК РФ // Журнал российского права. 2016. № 4. С. 107.

[379] См.: Интернет-ресурс «Судебные и нормативные акты РФ» – URL: https://sudact.ru/ (дата обращения: 23.05.2019).

Интернет (74 %). Остальная часть преступных деяний данной нормы приходится на незаконный сбыт специальных технических средств, предназначенных для негласного получения информации (26 %).

Сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ, для удобства читателя приведены в Приложении 9.

В юридической литературе высказана точка зрения о несоответствии тяжести наказания и последствий, причиненных в результате нарушения ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ. Только приобретение специальных технических средств без их незаконного использования не наносит какой-либо вред конституционным правам человека и гражданина[380]. Схожей точки зрения придерживается А. Б. Урпин, считающий, что приобретение без цели сбыта данных предметов не представляет значительной общественной опасности[381]. В целом мы поддерживаем данные позиции.

В связи с бурным развитием информационно-телекоммуникационных технологий появляются все новые и новые специальные технические средства, предназначенные для негласного получения

[380] См.: Кривогин М. С. Незаконный оборот специальных технических средств: проблемы квалификации преступлений // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. 2014. № 2. С. 111.

[381] Урпин А. Б. Совершенствование уголовной ответственности за незаконный оборот специальных технических средств, предназначенных для негласного получения информации // Уголовный закон России: пути развития и проблемы применения: сб. науч. статей / под ред. д-ра юрид. наук, профессора В. И. Тюнина. СПб.: Изд-во СПбГЭУ, 2013. С. 257.

информации. Они становятся все более миниатюрными, скрытными и технически совершенными[382].

По мнению С. П. Олефиренко, использование специальных технических средств, предназначенных для негласного получения информации о частной жизни граждан или деятельности юридических лиц, с последующим использованием полученной информации в преступных целях требует особой квалификации[383]. Это положение является спорным. Использование специальных технических средств значительно упрощает процесс перехвата информации и проникновения в тайну личной жизни, поэтому, по нашему мнению, данное обстоятельство должно являться квалифицирующим признаком преступления, предусмотренного ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ, и усиливать наказание.

Представляется, что в действующем УК РФ недостаточно учтена общественная опасность незаконного обращения со специальными техническими средствами, предназначенными для негласного получения информации. Видится, что, кроме ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ, они могут быть обозначены и в других нормах. Так, с помощью специальных технических средств, предназначенных для негласного получения информации, могут быть получены сведения, составляющие коммерческую или банковскую тайну (ст. 183 УК РФ), сведения о частной жизни человека (ст. 137 УК РФ),

---

[382] Бегишев И. Р. Уголовно-правовое нововведение в сфере защиты цифровой информации // Information Security / Информационная безопасность. 2011. № 1. С. 18.

[383] Олефиренко С. П. Уголовно-правовое исследование состояния морального вреда в преступлениях, предусмотренных статьями 138, 138.1 Уголовного кодекса Российской Федерации // Вестник Челябинского государственного университета. 2013. № 5. С. 93.

нарушена тайна переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ), нарушена тайна голосования (ст. 141 УК РФ). Аналогичной позиции придерживаются Т. М. Лопатина[384] и С. Д. Петроченков[385].

Ст. 141 «Воспрепятствование осуществлению избирательных прав или работе избирательной комиссии» УК РФ предусматривает ответственность за нарушение тайны голосования. Однако слежение за волеизъявлением гражданина с использованием специальных технических средств, предназначенных для негласного получения информации, имеет, по нашему мнению, повышенную опасность.

Предлагаем в связи с этим установить в качестве квалифицирующего признака ответственность за нарушение тайны голосования с использованием специальных технических средств, предназначенных для негласного получения информации.

Незаконное собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, ответственность за которое также установлена ст. 183 УК РФ, вполне может быть совершено с использованием специальных технических средств, предназначенных для негласного получения информации. Поэтому предлагаем установить в качестве квалифицирующего признака данного преступления ответственность за собирание сведений с использованием специальных технических средств, предназначенных для негласного получения информации.

---

[384] Лопатина Т. М. Совершенствование уголовно-правового регулирования использования специальных технических средств, предназначенных для негласного получения информации // Российское право: образование, практика, наука. 2018. № 4 (106). С. 76.

[385] См.: Петроченков С. Д. Квалификация способов совершения преступления, предусмотренного статьей 183 Уголовного кодекса Российской Федерации // Юристъ-Правоведъ. 2018. № 1 (80). С. 60; Петроченков С. Д. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну. М.: ЮНИТИ-ДАНА, 2017. С. 45.

Объективную сторону преступления, предусмотренного ст. 137 «Нарушение неприкосновенности частной жизни» УК РФ, образует в числе прочего незаконное собирание сведений о частной жизни, составляющих личную и семейную тайну другого лица. По основаниям, аналогичным изложенным выше, предлагаем установить в качестве квалифицирующего признака данного преступления незаконное собирание сведений о частной жизни, составляющих личную или семейную тайну другого лица, с использованием технических средств, предназначенных для негласного получения информации.

Следует при этом отметить, что использование специальных и иных технических средств, предназначенных для негласного получения информации, предусмотрено в качестве квалифицирующего признака преступления против основ конституционного строя и безопасности государства (ч. 2 ст. 283.1 «Незаконное получение сведений, составляющих государственную тайну» УК РФ). Таким образом, наши предложения о введении подобных квалифицирующих признаков в другие статьи УК РФ будут способствовать повышению системности российского уголовного закона.

Видится, что действенной мерой предупреждения распространения и применения специальных технических средств, используемых для негласного получения информации, является мера уголовно-правового запрета их обращения.

В целях ограничения оборота специальных технических средств, используемых для негласного получения информации, предлагается установить в ч. 1 ст. 226.1 «Контрабанда сильнодействующих, ядовитых, отравляющих, взрывчатых, радиоактивных веществ, радиационных источников, ядерных материалов, огнестрельного оружия или его основных частей, взрывных устройств, боеприпасов, оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а также материалов и оборудования, которые могут быть использованы при создании

оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а равно стратегически важных товаров и ресурсов или культурных ценностей либо особо ценных диких животных и водных биологических ресурсов» УК РФ ответственность за их контрабанду. Схожей позиции придерживается С. Д. Петроченков[386]. Представляется, что аналогичным образом можно ограничить оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

В целях государственного регулирования широкого круга правоотношений, возникающих при обороте специальных технических средств, используемых для негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации и предупреждения соответствующих деяний, представляется целесообразным принять отдельный федеральный закон «О специальных технических средствах».

В заключение параграфа сформулируем предложения, направленные на совершенствование норм уголовного законодательства за использование специальных технических средств, предназначенных для негласного получения информации, а также на ограничение оборота указанных средств:

– вместо термина «специальные технические средства, предназначенные для негласного получения информации» использовать в УК РФ более точный и недвусмысленный термин «*технические средства негласного получения информации*»;

– в примечании к ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ рекомендовано изложить определение поня-

[386] См.: Петроченков С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации: автореф. дис. … канд. юрид. наук. М., 2013. С. 10.

тия «техническое средство негласного получения информации» в следующей редакции: «*Под техническим средством негласного получения информации следует понимать программное либо аппаратное устройство, созданное или приспособленное для негласного перехвата, обработки и анализа информации*»;

– поскольку в УК РФ недостаточно учтена общественная опасность неправомерного обращения с техническими средствами негласного получения информации, предложено установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 2 ст. 137 «Нарушение неприкосновенности частной жизни», ч. 2 ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ, ч. 2 ст. 141 «Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий» и ч. 3 ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ;

– доказана целесообразность установления в ст. 226.1 «Контрабанда сильнодействующих, ядовитых, отравляющих, взрывчатых, радиоактивных веществ, радиационных источников, ядерных материалов, огнестрельного оружия или его основных частей, взрывных устройств, боеприпасов, оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а также материалов и оборудования, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а равно стратегически важных товаров и ресурсов или культурных ценностей либо особо ценных диких животных и водных биологических ресурсов» УК РФ ответственности за контрабанду специальных технических средств, используемых для негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, путем внесения

следующих дополнений в наименование ст. 226.1 УК РФ и в диспозицию ч. 1 ст. 226.1 УК РФ: после слов *«ядерных материалов»* указать *«технических средств негласного получения информации, специальных технических средств, предназначенных для нарушения систем защиты цифровой информации»*;

– в целях государственного регулирования правоотношений, возникающих при обороте технических средств негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации и предупреждения соответствующих деяний, аргументировано предложение о принятии отдельного федерального закона «О специальных технических средствах». В нем необходимо определить правила их оборота, содержание используемых понятий, субъекты, которым разрешено использовать указанные средства, установить порядок их применения и т. д.

§ 3.3. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации

Современные информационно-телекоммуникационные технологии кардинально и непрерывно изменяют нашу повседневную жизнь в лучшую сторону и вместе с тем создают все новые виды угроз огромному количеству охраняемых законом объектов. Одним из основных способов проникновения в информационно-телекоммуникационные устройства, системы и сети является неправомерный доступ к охраняемой законом цифровой информации, в том числе к сведениям, содержащим государственную, коммерческую, налоговую, банковскую, врачебную, профессиональную, личную, семейную или какую-либо иную тайну.

Следует четко понимать, что этап проникновения в информационно-телекоммуникационные устройства с целью, например, копирования информации наступает только после этапа обхода или нарушения системы защиты цифровой информации, предусмотренной в таких устройствах, иначе преступнику просто не удастся заполучить нужную ему конфиденциальную информацию.

Существующие информационно-телекоммуникационные устройства, системы и сети в основном хорошо защищены от атак на цифровую информацию, обращающуюся в них, так как находятся под охраной современных технических средств защиты цифровой информации.

Однако, как показывает практика, одновременно с разработкой технических средств защиты создаются технические средства, направленные на взлом (несанкционированный доступ к цифровому формату). С указанными нарушениями предлагается бороться существующими юридическими методами, подвергая преследованию лиц, которые разрабатывают, изготавливают или распространяют предназначенные для несанкционированного доступа устройства и программное обеспечение[387].

Безопасность цифровой информации может быть нарушена в нескольких случаях: во-первых, при получении неправомерного доступа к цифровой информации, во-вторых, при нарушении работы информационно-телекоммуникационного устройства, системы и сети, в-третьих, при действии вредоносных компьютерных программ. В основном системы защиты цифровой информации включают в себя следующие элементы: подсистемы защиты информационно-телекоммуникационного устройства, подсистемы защиты операционной системы и цифровых данных, а также подсистемы безопасности каналов передачи цифровой информации.

[387] Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. … д-ра юрид. наук. М., 2015. С. 95.

При неправомерном доступе к операционной системе компьютера наиболее уязвимыми элементами системы защиты у самой распространенной операционной системы – *Windows* – являются следующие:

– аутентификационные данные пользователей компьютера, хранящиеся в их системных реестрах, с которых они осуществляли вход в компьютер;

– системное программное обеспечение компьютеров[388].

На сегодняшний день наиболее актуальным является рассмотрение неправомерного доступа в операционную систему компьютера посредством преодоления парольной защиты на вход в операционную систему, т.е. проникновение через воздействие на подсистему аутентификации данных пользователей компьютера[389].

Исследователи приходят к выводу, что неправомерный доступ к операционной системе компьютера путем преодоления парольной защиты на вход в операционную систему компьютера бывает двух видов:

– неправомерный доступ к операционной системе компьютера посредством подбора паролей на вход в операционную систему компьютера;

– неправомерный доступ к операционной системе компьютера посредством сброса паролей на вход в операционную систему компьютера[390].

Рассмотрим два основных механизма совершения неправомерного проникновения в компьютер, связанного с преодолением парольной защиты на вход в операционную систему компьютера

---

[388] Ярочкин В. И. Информационная безопасность: учебник для вузов. М.: Летописец, 2000. С. 41.

[389] Радько Н. М., Язов Ю. К., Суховеров А. С. Угрозы непосредственного доступа в операционную среду компьютера // Информация и безопасность. 2007. № 2. С. 317.

[390] Там же. С. 318.

с помощью специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

Исследуем первый механизм проникновения в операционную систему компьютера с помощью специального технического средства, предназначенного для нарушения системы защиты цифровой информации. Основным методом является метод взлома парольной защиты операционной системы при помощи взломщиков паролей[391]. Представляется, что работа таких программ основана на нарушении предусмотренной защиты операционной системы от неправомерного доступа. Следовательно, указанная программа будет являться специальным техническим средством, предназначенным для нарушения систем защиты цифровой информации.

Рассмотрим второй механизм преодоления парольной защиты на вход в операционную систему компьютера посредством сброса паролей. Сброс паролей на вход в операционную систему компьютера – способ, при котором можно сбросить или изменить любой пароль. Для этого удобнее всего также использовать специальные программы. Осуществить сброс паролей на вход в операционную систему компьютера можно путем замены системной библиотеки на ее модифицированную версию, в которой отключена проверка пароля при авторизации пользователя в системе. Существуют и различные вирусы, изменяющие эти библиотеки автоматически[392].

Следует при этом отметить, что В. Б. Щербаков[393] в своей работе рассмотрел беспроводные информационно-телекоммуникационные сети в качестве объекта обеспечения информационной безопасности и провел их классификацию по набору применяемых средств защиты.

---

391 Там же. С. 318.

392 Там же. С. 320.

393 Щербаков В. Б. Классификация беспроводных сетей по набору применяемых средств защиты // Информация и безопасность. 2009. № 1. С. 126.

Рассмотрим пример применения специального технического средства, предназначенного для нарушения систем защиты цифровой информации в виде программы. Так, атака «*arp*-спуфинг» используется в локальной сети, построенной на коммуникаторах. Для ее реализации злоумышленник может воспользоваться такими программами, как *Ettercap*, *Cain&Abel*, причем в данных программах реализована обработка перехватываемой информации и выделение интересующих частей, таких как имя и пароль. Подобную атаку довольно сложно обнаружить, так как обычно злоумышленник находится внутри организации[394].

Средства защиты цифровой информации – это совокупность программных и аппаратных устройств, предназначенных для обеспечения безопасности цифровой информации. К средствам защиты информации можно отнести брандмауэры[395], учетные записи пользователей, антивирусное программное обеспечение, программно-аппаратные комплексы аутентификации и идентификации, устройства для ввода биометрических идентификационных признаков, средства защиты информации от неправомерного доступа, средства обнаружения атак, средства анализа защищенности, средства криптографической защиты информации и т. д.

Доступ к информационным ресурсам компьютера пользователь получает после успешного выполнения процедур идентификации и аутентификации. Идентификация заключается в распознавании пользователя по присущему или присвоенному ему идентификационному признаку. Проверка принадлежности предъявленного

---

394 Радько Н. М., Язов Ю. К., Суховеров А. С. Указ. раб. С. 311.

395 Брандмауэр – это программный и/или аппаратный барьер между двумя сетями, позволяющий устанавливать только авторизованные межсетевые соединения. Брандмауэр защищает соединяемую с Интернетом корпоративную сеть от проникновения извне и исключает возможность доступа к конфиденциальной информации.

им идентификатора (подтверждение подлинности) проводится в процессе аутентификации[396].

Следует отметить, что все средства, предназначенные для нарушения систем защиты цифровой информации, подразделяются на аппаратные и программные. В свою очередь средства защиты цифровой информации также подразделяются на аппаратные и программные.

В соответствии с утвержденной решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. действующей «Концепцией защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации»[397] к основным способам несанкционированного доступа к информации относятся:

– непосредственное обращение к объектам доступа;

– создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты информации;

– модификация средств защиты информации, позволяющая осуществить несанкционированный доступ;

– внедрение в технические средства вычислительной техники или автоматизированных систем программных или технических механизмов, нарушающих предполагаемую структуру и функции средств вычислительной техники и автоматизированных систем и позволяющих осуществить несанкционированный доступ.

Во многих случаях неправомерные деяния с цифровой информацией невозможны без использования специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. Основное назначение таких специальных техниче-

[396] Рычкалова Л. А., Нарижный А. В. Биометрические средства идентификации // Вестник МГОУ. Серия «Юриспруденция». 2008. № 3. С. 38.

[397] Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». М.: ГТК РФ, 1992. С. 7.

ских средств – это взлом или обход имеющихся средств защиты цифровой информации в информационно-телекоммуникационных устройствах, их системах и сетях.

К числу специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, можно отнести следующие: сканеры портов информационно-телекоммуникационных устройств, программное обеспечение, предназначенное для дешифрования цифровой информации и для подбора паролей аутентификации, вредоносные компьютерные программы и т. д.

Появление генераторов вирусов позволяет, задав программе-генератору в виде входных параметров способ распространения, тип, вызываемые эффекты, причиняемый вред, получить текст нового вируса[398]. Такие генераторы представляются крайне опасными.

В. С. Карпов считает, что одним из способом совершения рассматриваемых преступлений могут служить изготовление и сбыт специальных средств для получения несанкционированного доступа к компьютерной системе или сети[399]. Позиция данного исследователя представляется не совсем удачной ввиду неточного определения сути предмета и обобщения воедино всех специальных средств для получения несанкционированного доступа, которых много очень разных, а также отсутствия подробной классификации названных специальных средств. Но следует согласиться с автором, что сама проблема существует и весьма серьезна, так как данные специальные средства мешают нормальному развитию общественных отношений в сфере цифровой информации.

---

[398] Зегжда П. Д. Современные аспекты обеспечения безопасности информационно-телекоммуникационных систем // Проблемы информационной безопасности. Компьютерные системы. 2002. № 1. С. 14.

[399] Карпов В. С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юрид. наук. Красноярск, 2002. С. 98.

К сожалению, в настоящий момент в сети Интернет находится огромный массив общедоступных программ, предназначенных для нарушения систем защиты цифровой информации, и каждый пользователь Сети может получить их совсем просто. Всеобщая распространенность таких специальных технических средств чревата трагическими последствиями[400].

На наш взгляд, более точным и правильным решением данной проблемы стала бы криминализация оборота специальных технических средств, предназначенных для нарушения систем защиты цифровой информации и проникновения в информационно-телекоммуникационные устройства, системы и их сети.

Кроме того, А. Ю. Чупрова указывает на целесообразность введения в уголовное законодательство нормы об ответственности за производство, продажу, приобретение, владение с целью использования для совершения запрещенных в законе действий, компьютерных программ, разработанных или адаптированных, компьютерных паролей, кодов доступа или иных аналогичных инструментов, с помощью которых может быть получен незаконный доступ к компьютерной системе в целом или любой ее части[401]. Приведенная точка зрения, несомненно, заслуживает поддержки.

Приведем следующий пример. Так, гр. К. умышленно осуществлял подключения к сети Интернет, используя чужие учетные записи. С помощью специальных компьютерных программ – сканера двойного назначения и программы подбора паролей, в целях подключения к сети Интернет – он незаконно получал логины и пароли, принадлежащие ОАО «РЕСО-Гарантия» (г. Новотроицк) и Управлению судебного департамента при Верховном суде Рос-

[400] Бегишев И. Р. Преступления в сфере цифровой информации: состояние, пробелы и пути их решения // Информационное право. 2010. № 2. С. 20.

[401] Чупрова А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. … д-ра юрид. наук. М., 2015. С. 70.

сийской Федерации в Оренбургской области. В результате услуги интернет-провайдера, которыми пользовался гр. К., оплачивались за счет средств указанных юридических лиц[402].

В УК РФ термин «специальные технические средства» упоминается в ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ. Среди обстоятельств, отягчающих наказание, в п. «к» ч. 1 ст. 63 УК РФ, как уже было отмечено выше, предусмотрено совершение преступления с использованием в числе прочего, специально изготовленных технических средств. Традиционно под такими предметами понимались отмычки и другой воровской инструмент, который изначально разрабатывался и применялся для совершения преступлений. Например, для краж со взломом. Но нет причин отказываться понимать круг таких предметов шире.

Пункт «а» ч. 3 ст. 243.2 «Незаконные поиск и (или) изъятие археологических предметов из мест залегания» в качестве особо квалифицированного состава называет совершение деяния с использованием специальных технических средств поиска и (или) землеройных машин. В примечании 2 к этой же статье приведено определение понятия указанных средств: «Под специальными техническими средствами поиска в настоящей статье понимаются металлоискатели, радары, магнитные приборы и другие технические средства, позволяющие определить наличие археологических предметов в месте залегания». Здесь категория «специальности» понимается как пригодность для осуществления такой функции, как «определение наличия археологических предметов в месте залегания». О предназначенности здесь речи нет.

Наконец, п. «г» ч. 2 ст. 283.1 «Незаконное получение сведений, составляющих государственную тайну» устанавливает повышенную

[402] В Оренбуржье вынесен приговор хакеру // Информационное агентство Regnum. URL: http://regnum.ru/news/accidents/1257598.html (дата обращения: 23.05.2019).

ответственность за совершение данного деяния с использованием специальных и иных технических средств, предназначенных для негласного получения информации.

Необходимо отметить, что в ряде действующих нормативных актов используется родовое понятие «специальные технические средства», которое до сих пор не определено на законодательном уровне, и это обстоятельство в некоторых случаях создает проблемы. Неопределенный или не четко определенный понятийный аппарат порождает ситуации, когда под одним и тем же термином подразумевается различное содержание или, наоборот, когда под разными терминами скрывается одно и то же. Как указывают исследователи, в действующем законодательстве не только не выработаны единые принципы регламентации применения технических средств при проведении оперативно-розыскных мероприятий и процессуальных действий, но и не определены общие понятия и термины[403].

Следует отметить, что с помощью специальных технических средств может осуществляться радиоперехват информации, а с помощью специальных технических средств, предназначенных для нарушения систем защиты цифровой информации,– неправомерный доступ к компьютерной информации.

В ст. 6 «Оперативно-розыскные мероприятия» Федерального закона «Об оперативно-розыскной деятельности» запрещено проведение оперативно-розыскных мероприятий и использование специальных и иных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации, неуполномоченными на то

[403] Лахов В. Г., Ковалев С. Д., Полуянова Е. В. Содержание понятия «специальные технические средства» в оперативно-розыскной деятельности: научные и нормативные подходы // Вестник Международного юридического института. 2016. № 1. С. 38.

настоящим федеральным законом физическими и юридическими лицами[404].

Аналогичным образом необходимо установить запрет на использование специальных технических средств, предназначенных для нарушения систем защиты цифровой информации. Однако мы полагаем, что использование таких специальных технических средств может быть направлено и на решение специальных задач правоохранительных органов.

Следует отметить, что нормы ответственности за незаконное обращение таких средств присутствуют и в зарубежном уголовном законодательстве. Так, в ст. 361.1 «Создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт» Уголовного кодекса Украины предусмотрена ответственность за создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт[405].

Кроме того, в ст. 278.3 «Изготовление с целью сбыта либо сбыт и распространение специальных средств для получения незаконного (несанкционированного) доступа к компьютерной системе, а также к сетям телекоммуникаций» Уголовного кодекса Республики Узбекистан предусмотрена ответственность за изготовление с целью сбыта либо сбыт и распространение специальных средств для получения несанкционированного доступа к компьютерной системе[406].

Необходимо подчеркнуть, что в ст. 323.3.1 Уголовного кодекса Французской Республики предусмотрена ответственность за импорт, хранение, предложение, передачу или предоставление оборудования,

---

[404] Об оперативно-розыскной деятельности: Федеральный закон № 144-ФЗ от 12 августа 1995 г. // СЗ РФ. 1995. № 33. Ст. 3349.

[405] См.: Уголовный кодекс Украины. URL: http://kodeksy.com.ua/ka/ugolovnyj_kodeks_ ukraini.htm (дата обращения: 23.05.2019).

[406] См.: Уголовный кодекс Республики Узбекистан. URL: http://fmc.uz/legisl.php?id=k_ug (дата обращения: 23.05.2019).

инструмента, компьютерных программ или данных, разработанных или специально приспособленных для совершения посягательств на системы автоматизированной обработки данных[407].

Особо следует отметить, что специальные технические средства, предназначенные для нарушения систем защиты цифровой информации, могут быть созданы из исследовательского интереса в личных целях для дальнейшего научного изучения и разработки средств защиты цифровой информации. Представляется, что такое производство специальных технических средств, если оно не направлено на реальное нарушение систем защиты цифровой информации, не должно преследоваться по закону.

Поскольку оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, имеет повышенную опасность, предлагаем следующее:

– установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 3 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ и в ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ;

– ввести отдельную норму об ответственности за незаконные производство, приобретение и (или) сбыт таких средств в следующей авторской редакции:

> *«Статья 273.1. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации*
> *1. Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для нарушения систем защиты цифровой информации,–*

[407] См.: Уголовный кодекс Французской Республики. URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата обращения: 23.05.2019).

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения,–

наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

Представляется, что введение такой нормы позволит дифференцировать ответственность и закроет существующий в уголовном законодательстве пробел.

§ 3.4. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем

Современный век высоких технологий немыслим без оперативного обмена цифровой информацией. Цифровая информация окружает нас повсюду: во время работы за компьютером, при передаче данных в системах мобильной связи, при работе с использованием беспроводных технологий передачи данных, в информационно-телекоммуникационной сети Интернет и т. д.

Следует отметить, что порой цифровая информация является не только объектом преступных посягательств, но и объектом экономической деятельности[408].

Согласно данным аналитического центра российской компании *InfoWatch*, крупнейшего российского производителя решений для защиты организаций от внутренних и внешних угроз, а также от информационных атак, в 2018 г. было зарегистрировано 2 263 случая утечек конфиденциальной информации из организаций: из них 77,2 % – из коммерческих организаций, 22,8 % – из государственных организаций. По типу информации все утечки распределяются на следующие виды: персональные данные – 69,5 %, платежная информация – 16,9 %, коммерческая тайна – 8,1 %, государственная тайна – 5,4 % от числа всех зафиксированных утечек. Данные о вышесказанных утечках конфиденциальной информации включают все инциденты во всех зарубежных странах, информация о которых была опубликована в средствах массовой информации, а также в блогах, на веб-форумах и других сетевых ресурсах[409].

Российский уголовный закон знает несколько преступлений, субъект которых незаконно поступает в отношении полученных преступным путем ценностей. Это легализация (отмывание) денежных средств или иного имущества, приобретенных другими лицами преступным путем (ст. 174 УК РФ), легализация (отмывание) денежных средств или иного имущества, приобретенных лицом в результате совершения им преступления (ст. 174.1 УК РФ), приобретение или сбыт имущества, заведомо добытого преступным

---

[408] Бегишев И. Р. Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем // Безопасность информационных технологий. 2010. № 1. С. 43.

[409] Аналитический отчет «Глобальное исследование утечек конфиденциальной информации в 2018 г.» // Аналитический центр InfoWatch. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1 (дата обращения: 23.05.2019).

путем (ст. 175 УК РФ), незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну (ст. 183 УК РФ), государственная измена в форме шпионажа (ст. 275 УК РФ) и собственно сам шпионаж (ст. 276 УК РФ).

Ограничение оборота цифровой информации, заведомо добытой преступным путем, как представляется, является ключевым средством противодействия преступлениям в сфере высоких технологий и, несомненно, нуждается в уголовно-правовой защите[410].

Постоянные предложения приобрести различные (в большинстве своем ведомственные или корпоративные) базы данных свидетельствуют о том, что продажа конфиденциальных сведений о гражданах и юридических лицах стала отдельным видом бизнеса. Если появление очередной опубликованной базы для граждан является просто еще одним малоприятным фактом обнародования сведений об их частной жизни, то для некоторых предприятий это может оказать отрицательное влияние на бизнес-процессы. Например, для оператора сотовой связи распространение базы биллинга может обернуться существенным оттоком абонентов к более «надежному» оператору-конкуренту. Поэтому оператору подчас экономически более выгодно найти «производителя», подготовившего украденную базу к продаже, и выкупить весь тираж. Но проблема перекрытия возможных утечек при этом остается весьма актуальной[411].

Часто цифровая информация, циркулирующая в информационно-телекоммуникационных устройствах, их системах и сетях, становится объектом преступных посягательств. Похищенная цифровая информация передается, например, заказчику за возна-

[410] Бегишев И. Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем // Актуальные проблемы экономики и права. 2010. № 1. С. 123.

[411] Сабанов А. Безопасность баз данных // Connect! 2006. № 4. С. 14.

граждение. Примерами соответствующих правонарушений могут служить следующие деяния:

– перехват, запись на носитель цифровой информации или сбыт полученной цифровой информации;

– кража или вымогательство цифровой информации о клиентах организаций, кража персональных данных или кредитных историй граждан с целью их последующей реализации или использования в незаконных целях.

Так, в Соединенном Королевстве Великобритании и Северной Ирландии вынесен приговор программисту, пытавшемуся продать секретные сведения. Д. Хоутон, работая на *MI*6 в должности инженера-программиста, скопировал на *USB*-носитель более 7 тыс. файлов, содержащих список сотрудников *MI*6, работающих за границей. Хоутон пытался продать данные спецслужбам Королевства Нидерланды за 1 млн фунтов, однако потенциальные покупатели незамедлительно связались со своими коллегами из Соединенного Королевства, приняв данное предложение за попытку мошенничества[412].

В Республике Корея задержаны трое лиц, сбывавших не подлежащие огласке сведения: пароли и адреса, принадлежащие более 20 млн соотечественников. Арестованные приобрели данные у хакеров из Китайской Народной Республики[413].

Существенным пробелом в УК РФ является отсутствие нормы, устанавливающей ответственность за приобретение или сбыт циф-

---

[412] Аникеенко В. Вынесен приговор программисту, пытавшемуся продать секретные сведения // Аналитика по информационной безопасности Anti-Malware.ru. [Электронный ресурс]. – URL: https://www.anti-malware.ru/news/2015-12-21/2908 (дата обращения: 23.05.2019).

[413] Панасенко А. В Южной Корее обнаружена самая большая в истории страны утечка личных данных // Аналитика по информационной безопасности Anti-Malware.ru. [Электронный ресурс]. – URL: https://www.anti-malware.ru/news/2015-12-21/2325 (дата обращения: 23.05.2019).

ровой информации, заведомо добытой преступным путем, так как последняя не подпадает под признаки ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ[414] и других перечисленных выше норм.

Предметом преступления, предусмотренного в ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ, выступает имущество, заведомо добытое преступным путем. К имуществу обычно относят движимое и недвижимое имущество, различные вещи и т.д.

Законодатель указывает, что имущество, выступающее в качестве предмета преступления, должно быть добыто преступным путем. Способами такой добычи являются, прежде всего, хищения, вымогательство, получение взятки, коммерческий подкуп, незаконное получение кредита, подкуп участников и организаторов спортивных соревнований и т.д.

Также предметами преступления, предусмотренного ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ, не могут быть драгоценные металлы, природные драгоценные камни, ядерные материалы или радиоактивные вещества, оружие, взрывчатые вещества, наркотические средства или психотропные вещества, сильнодействующие или ядовитые вещества. Их незаконное приобретение наказывается, соответственно, по ст. 191 «Незаконный оборот драгоценных металлов, природных драгоценных камней или жемчуга», 220 «Незаконное обращение с ядерными материалами или радиоактивными веществами», 222 «Незаконные приобретение, передача, сбыт, хранение, перевозка или ношение оружия, его основных частей, боеприпасов», 228 «Незаконные приобретение, хранение, перевозка, изготовление, переработка наркотических средств, психотропных веществ или их

[414] Бегишев И. Р. Противодействие утечкам цифровой информации: вопросы уголовной ответственности // Защита информации. Inside. 2011. № 2. С. 33.

аналогов, а также незаконные приобретение, хранение, перевозка растений, содержащих наркотические средства или психотропные вещества, либо их частей, содержащих наркотические средства или психотропные вещества», 234 «Незаконный оборот сильнодействующих или ядовитых веществ в целях сбыта» УК РФ.

Информацию обычно не признают имуществом, и поэтому манипуляции с ней не подпадают под действие ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ, так как в названной норме под имуществом понимается совокупность вещей и материальных ценностей, находящихся во владении или законном пользовании физического или юридического лица. Думается, что цифровая информация имеет некоторую схожесть с материальными ценностями, поскольку важна для обладателя и характеризуется рядом эффектов. Однако между ними имеется принципиальное различие: цифровую информацию, по сравнению, например, с драгоценным металлом или ценной бумагой, являющимися материальными ценностями, невозможно потрогать и ощутить, хотя носитель информации (например, флеш-карта), на котором находится цифровая информация, является материальной ценностью. Компьютер в этом случае будет являться предметом преступления, предусмотренного ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ.

К аналогичным выводам приходит Т. М. Лопатина, считающая, что информация – это не имущество, она не обладает экономическим, социальным и юридическим признаками, характеризующими чужое имущество как предмет хищения. Это всего лишь сведения, представленные в специфической форме[415].

[415] Лопатина Т. М. Проблемы уголовно-правовой защиты сферы компьютерной информации: современный взгляд на мошенничество // Право и безопасность. 2013. № 3–4. С. 93.

Следует отметить, что законодателем в качестве отдельного вида вещественных доказательств по уголовным делам выделены электронные носители информации[416].

Довольно интересной представляется точка зрения А. С. Крапивенского, предлагающего считать информацию товаром и утверждающего, что в XXI столетии информация переходит в раздел наиболее востребованных товаров, предлагаемых к продаже или обмену[417].

Сначала он предлагает определить само понятие «информация», позволяющее считать ее товаром. Словарь трактует ее как «сведения о лицах, предметах, событиях, явлениях, процессах и объектах (независимо от формы их представления), используемые в целях оптимизации принятия решений и управления объектами». Разумеется, в условиях рыночной экономики сведения, используемые для оптимизации принятия решений и управления объектами, являются не чем иным, как товаром. Однако собственно «информация» является не совсем обычным товаром. Это отмечает, в частности, Р. Дж. Нолл: «Информацию необходимо каким-то образом доводить до последующих потребителей, и распространение ее может даже стоить дороже, чем повторное создание,– это, например, относится к простейшим компьютерным программам. Или, например, информацию можно приватизировать, причем стоить это будет очень недорого, так что свойство информации служить общественным благом не внесет значительной неэффективности в систему ее рыночного распространения. Тем не менее публичность информации – это серьезная проблема»[418].

---

416 См.: Уголовный процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // СЗ РФ. 2001. № 52 (ч. I). Ст. 4921.

417 Крапивенский А. С. Информация как товар в XXI веке: анализ угроз безопасности национальным рынкам // Информационная безопасность 2010: материалы VII Международной конференции, 15–16 апреля 2010 г. Кишинев, 2010. С. 15.

418 Там же.

Как считает О. Н. Крапивина, имущество, согласно ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ, состоит из вещей, индивидуально определенных и определенных родовыми признаками, потребляемых и непотребляемых; одушевленных и неодушевленных. В силу нематериального происхождения к предмету преступного приобретения (сбыта) по российскому уголовному закону также не могут быть отнесены идеи, взгляды, информация, компьютерная информация, электрическая и тепловая энергия[419].

Несомненно и то, что цифровая информация, выступающая в качестве предмета преступления, должна быть добыта преступным способом.

Предполагается, что преступными являются способы добычи цифровой информации, предусмотренные ст. 272 «Неправомерный доступ к компьютерной информации» и 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ. Так, неправомерный доступ к компьютерной информации может повлечь за собой копирование информации, а распространенная в информационно-телекоммуникационной сети вредоносная компьютерная программа может найти, скопировать и переслать ценную информацию в чужие руки.

Сегодня стремительно и динамично развиваются системы беспроводной связи, позволяющие передавать на большие расстояния не только голосовую информацию, но и визуальную в виде графики и видео. Циркулирующая в этих системах цифровая информация может содержать конфиденциальные данные, сведения о личной и семейной жизни, банковскую и налоговую тайны и т. д.

---

[419] Крапивина О. Н. Приобретение или сбыт имущества, заведомо добытого преступным путем: сравнительно-правовое, уголовно-правовое, уголовно-политическое и криминологическое исследование: автореф. дис. … канд. юрид. наук. М., 2008. С. 12.

Следует отметить, что с расширением объема коммерческой деятельности в сети Интернет личные данные, позволяющие установить наиболее важные сведения о человеке, приобретают все большую ценность, а ущерб, который может быть причинен путем использования персональной информации, связан не только с прямыми имущественными потерями, но и с упущенной выгодой, негативными социальными последствиями, организационным вредом, подрывом деловой репутации[420].

А. А. Шутова считает, что незаконное получение чужих регистрационных данных для доступа в информационно-телекоммуникационную сеть Интернет необходимо признавать собиранием сведений, составляющих коммерческую тайну, и в таких случаях дополнительно квалифицировать деяние по ч. 1 ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ[421]. В обществе с бурным развитием науки и техники складываются особые информационные отношения, предметом которых выступает информация[422], в том числе цифровая.

В современном информационном обществе, в котором информационно-телекоммуникационные системы охватывают все сферы деятельности человека, общества и государства, огромная роль отводится безопасности цифровой информации, обращающейся в этих системах.

Наряду со стремительным развитием современных информационно-телекоммуникационных систем обращения цифровой

---

[420] Чупрова А. Ю. Уголовно-правовая оценка мошенничества // Ученые труды Российской академии адвокатуры и нотариата. 2015. № 1. С. 69.

[421] Шутова А. А. Особенности квалификации незаконного получения сведений, составляющих коммерческую или банковскую тайну // Расследование преступлений: проблемы и пути их решения. 2016. № 3 (13). С. 76.

[422] Шутова А. А. Сравнительно-правовой анализ норм об ответственности за информационные преступления по законодательству Республики Казахстан и России // Наука. Мысль. 2016. № 9. С. 143.

информации, таких как беспроводные и волоконно-оптические системы, преступные сообщества применяют новые способы совершения противоправных деяний, направленных на завладение конфиденциальной цифровой информацией.

Все это делает актуальной задачу обеспечения безопасности цифровой информации, обращающейся в беспроводных информационно-телекоммуникационных системах.

На данный момент существует несколько способов совершения противоправных деяний в информационно-телекоммуникационных системах. Так, по мнению специалистов, наиболее опасными являются такие способы совершения преступлений, как перехват цифровой информации и неправомерный доступ к цифровой информации.

Согласно позиции В. Б. Вехова, способы совершения рассматриваемых видов преступлений делятся в зависимости от их вида на следующие: 1) компьютерная техника выступает в роли объекта посягательства; 2) она же выступает в роли орудия и средства совершения преступления. Подразумевая в первом случае то, что объектом преступного посягательства является информация, находящаяся в компьютере, и что несанкционированный доступ и манипулирование ею возможно с использованием средств компьютерной техники, указанный автор не отрицает того, что такие же действия могут быть совершены и без нее (например, физическое уничтожение жесткого диска компьютера с находящейся на нем информацией). Если орудием преступления является компьютерная техника, В. Б. Вехов подразумевает использование ее не только для получения несанкционированного доступа, прослушивания и перехвата сообщений и т. п., но и для хранения преступной информации[423].

В отношении наиболее распространенных мошеннических схем при использовании сетевых ресурсов в сфере компьютерной

[423] Вехов В. Б. Компьютерные преступления: способы совершения методики расследования. М.: Право и закон, 1996. С. 26.

информации вряд ли возможно установить все способы мошенничества, сведя их к одному классификационному основанию. Однако вполне уместно говорить о типологии способов мошенничества, связанных с компьютерной информацией: например, мошенничество с виртуальными деньгами, инвестициями, товарообменом, лжеуслугами и благотворительностью, а также распространение вредоносных компьютерных программ с последующим извлечением материальной выгоды и т. п[424].

Рассмотрим способы совершения противоправных деяний в волоконно-оптических системах обращения цифровой информации. Они по своей структуре и принципу работы обеспечивают высокий уровень защиты от несанкционированного съема передаваемой информации. В то же время в волоконно-оптических системах имеется ряд возможностей несанкционированного съема информации. К ним, в частности, относятся пассивный распределенный несанкционированный доступ и пассивный локальный несанкционированный доступ[425].

В связи с высокой скоростью передачи информации и использованием оптических волокон с малым коэффициентом затухания пассивный распределенный несанкционированный доступ практически исключен для современных волоконно-оптических систем передачи информации.

В то же время особенно опасным способом съема информации с волоконно-оптической системы обращения цифровой информации является способ физического локального воздействия на оптическое волокно и отвода части оптического сигнала, распространяющегося по нему. Такой вид съема информации называется пассивным локальным несанкционированным доступом.

---

[424] Коломинов В. В. О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. 2015. № 3. С. 145.

[425] Румянцев К. Е., Хайров И. Е. Защита информации, передаваемой по световодным линиям связи // Информационное противодействие угрозам терроризма. 2004. № 2. С. 27–32.

На протяжении всей длины оптического волокна злоумышленник может успешно осуществлять практически не обнаруживаемый несанкционированный доступ к цифровой информации с помощью, например, специальных технических средств, предназначенных для негласного получения информации, и осуществлять запись информации, циркулирующей в волоконно-оптической системе обращения цифровой информации.

Для совершения противоправного деяния способом пассивного локального несанкционированного доступа злоумышленники обычно совершают три основных действия:

– выводят оптический сигнал из оптического волокна путем изгиба кабеля;

– принимают оптический сигнал на фотоприемник устройства несанкционированного доступа;

– преобразовывают оптический сигнал в цифровую информацию[426].

В то же время А. Ю. Карамнов указывает, что в момент передачи сведений по волоконно-оптической системе, исходя из примечания к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, их нельзя назвать компьютерной информацией, поэтому противоправные действия, совершаемые злоумышленником с использованием в качестве канала передачи данных волоконно-оптической системы, могут, исходя из строгого толкования нормы, препятствовать применению ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ[427]. Таким образом, определение компьютерной

[426] Бегишев И. Р. О некоторых способах совершения противоправных деяний в современных информационно-телекоммуникационных системах обращения цифровой информации // Информация и безопасность. 2009. № 4. С. 608.

[427] Карамнов А. Ю. Ответственность за создание, использование и распространение вредоносных компьютерных программ по действующему уголовному законодательству // Социально-экономические явления и процессы. 2012. № 11. С. 285.

информации, указанное в примечании к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, не является полным и исчерпывающим, что подтверждает наши выводы по поводу применения в статьях УК РФ термина «цифровая информация».

Несанкционированному доступу также подвержены беспроводные системы обращения цифровой информации из-за уязвимостей в протоколах обмена.

Существует множество вредоносных компьютерных программ, специально разработанных для взлома беспроводных систем и доступных в информационно-телекоммуникационной сети Интернет. Работа таких вредоносных компьютерных программ основана на перехвате сетевых пакетов, их анализе для получения пароля доступа с последующим раскодированием перехваченной цифровой информации.

В беспроводных системах обращения цифровой информации одним из основных общественно опасных способов завладения цифровой информацией является ее перехват, так как в отличие от проводных систем передачи информации, которые могут быть атакованы только лишь из информационно-телекоммуникационной сети Интернет, беспроводные системы доступны для противоправных деяний со стороны злоумышленников ввиду специфики распространения информации в пространстве.

Существует и иной способ добычи цифровой информации, не предусмотренный УК РФ,– это перехват цифровой информации, распространяющейся посредством радиоволн в пространстве. К ней можно отнести все правонарушения, посягающие на сведения, циркулирующие в современных сетях передачи данных, таких как *Wi-Fi*, *Bluetooth* и подобных.

Простая радиостанция стоимостью в пару сотен долларов позволит перехватывать многие конфиденциальные передачи. Обычно «говорят» при помощи азбуки Морзе, но также используют и человеческий голос, а в последнее время много информации

передают в «компьютерном» варианте. Конечно, радиоперехват не имеет никакого отношения к локальным сетям, но от этого его популярность не уменьшается. В эфире можно услышать много такого, что не найдешь ни на одном из серверов[428].

Более подробно вопросы уголовно-правовой регламентации перехвата цифровой информации были рассмотрены ранее.

Тем или иным преступным путем добытая цифровая информация может быть успешно сбыта или приобретена. Незаконное копирование такой информации наносит реальный материальный ущерб ее собственнику или владельцу.

На практике зачастую к такой информации в цифровой форме относят коммерческую тайну, персональные данные и т. д.

Так, А. Ю. Чупрова предлагает ввести уголовно-правовой запрет на хищение персональных данных и иной идентифицирующей информации, расположив новую норму в гл. 28 «Преступления в сфере компьютерной информации» УК РФ[429]. А. А. Шутова считает необходимым предусмотреть уголовную ответственность за незаконный сбор и (или) распространение информации (персональных данных) гражданина без его согласия[430]. Считаем такие предложения вполне оправданными.

Следует отметить, что в ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», 283 «Разглашение государственной тайны» УК РФ указаны виды

---

428 Касперский К. Взлом Пентагона. Как взломать закрытую сеть // Спецхакер. 2005. № 10. С. 75.

429 Чупрова А. Ю. Уголовно-правовая оценка мошенничества // Ученые труды Российской академии адвокатуры и нотариата. 2015. № 1. С. 70.

430 Шутова А. А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2015. № 4 (32). С. 334.

тайн, которые защищены законом, однако уголовная ответственность за приобретение и сбыт таких сведений, заведомо добытых преступным путем, в них не установлена.

Представляется необходимым отграничить преступные действия, связанные с приобретением и сбытом цифровой информации заведомо преступным путем, от деяний, предусмотренных ст. 146 «Нарушение авторских и смежных прав» и 147 «Нарушение изобретательских и патентных прав» УК РФ.

Необходимо сказать, что, помимо цифровой информации, незаконные действия с документированной информацией также могут нанести гражданам и организациям непоправимый ущерб. Например, кража ценных бумаг, платежных документов, бизнес-планов и иных документов, составляющих сведения конфиденциального характера, могут отрицательно повлиять на репутацию организации.

Ярким примером такого явления может послужить следующее событие: конфиденциальная медицинская информация пациентов одного из дорогих частных госпиталей Соединенного Королевства Великобритании и Северной Ирландии была продана сыщикам, работавшим под прикрытием. Сотни документов, содержащих личную информацию о состоянии здоровья пациентов, домашние адреса и даты рождения предлагались по $4 за каждый[431].

Проблемы применения уголовного законодательства в связи с развитием новых направлений в медицине, в частности применения электронной медицинской карты были подробно рассмотрены А. Ю. Чупровой[432].

---

[431] Великобритания: данные пациентов продаются на черном рынке // Английская ежедневная газета Daily Mail. URL: http://www.dailymail.co.uk/ news/article-1221186/Private-medical-records-sale-Harley-Street-clinic-patients-files-outsourced-input--end-black-market.html (дата обращения: 23.05.2019).

[432] Чупрова А. Ю. Проблемы использования электронных медицинских карт: уголовно-правовые аспекты // Ученые труды Российской академии адвокатуры и нотариата. 2014. № 4. С. 48.

В литературе высказана точка зрения о принципиальных отличиях между электронным[433] и бумажным документом. Интересной представляется позиция М. А. Ефремовой, предлагающей включить в УК РФ специальные составы, предусматривающие ответственность за незаконные деяния с электронными документами. В частности, она предлагает включить в ст. 292 «Служебный подлог», 324 «Приобретение или сбыт официальных документов и государственных наград», 325 «Похищение или повреждение документов, штампов, печатей либо похищение акцизных марок, специальных марок или знаков соответствия» и 327 «Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков» УК РФ нормы, содержащие новые составы преступлений, в качестве предметов которых выступают электронные документы[434].

Принимая во внимание результаты исследования И. П. Семченкова, считающего необходимым исключить из диспозиции ч. 1 ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ слова «заранее не обещанные»[435], мы по аналогичным соображениям предлагаем свою версию нормы ответственности за приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем.

Учитывая, что ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ не содержит указаний на такой предмет, как цифровая информация, предлагается установить уголовную ответственность за приобретение или сбыт

---

433 См.: например, Ефремова М. А. Уголовно-правовая охрана сведений, составляющих коммерческую, банковскую и налоговую тайны // Вестник Пермского университета. Юридические науки. 2015. № 1 (27). С. 127.

434 Ефремова М. А. Электронный документ как предмет преступления // Вестник Академии Генеральной прокуратуры Российской Федерации. 2015. Т. 49. № 5. С. 14.

435 Семченков И. П. Проблемы квалификации заранее обещанных укрывательства и приобретения или сбыта имущества, заведомо добытого преступным путем // Уголовное право. 2007. № 3. С. 59.

цифровой информации, заведомо добытой преступным путем, и дополнить УК РФ ст. 272.1 в следующей редакции:

> *«Статья 272.1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем*
> *1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем,–*
> *наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.*
> *2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения,–*
> *наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».*

Подводя итоги третьей главы исследования, предлагаем следующие выводы:

1. Предложены механизмы, направленные на совершенствование нормы, предусматривающей ответственность за мошенничество в сфере компьютерной информации, и некоторые механизмы противодействия такому мошенничеству:

– поскольку деяние, предусмотренное ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, относится к преступлениям в сфере обращения цифровой информации и со-

вершается с ее использованием, то указанную статью предлагается назвать «Мошенничество с использованием цифровой информации»;

– аргументировано, что мошенническое программное обеспечение относится к категории вредоносных цифровых программ. Уголовная ответственность за создание, использование и распространение мошеннического программного обеспечения (мошеннических программ) должна наступать по ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ;

– с целью дифференциации ответственности за мошенничество в сфере цифровой информации предлагается внести следующее дополнение в ч. 2 ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ: после слов *«значительного ущерба гражданину»* указать *«или с нарушением системы защиты цифровой информации»;*

– поскольку информационно-телекоммуникационная сеть Интернет содержит интернет-ресурсы, размещающие информацию о вредоносных компьютерных программах и программных средствах, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «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» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом:

> *«ж) вредоносных программ и программных средств, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей».*

2. Предложены механизмы, направленные на совершенствование норм уголовного законодательства за использование специальных технических средств, предназначенных для негласного получения информации, а также некоторые механизмы ограничения их оборота:

– вместо термина «специальные технические средства, предназначенные для негласного получения информации» использовать в УК РФ более точный и недвусмысленный термин «технические средства негласного получения информации»;

– в примечании к ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ рекомендовано изложить определение понятия «техническое средство негласного получения информации» в следующей редакции: «Под техническим средством негласного получения информации следует понимать программное либо аппаратное устройство, созданное или приспособленное для негласного перехвата, обработки и анализа информации»;

– поскольку в УК РФ недостаточно учтена общественная опасность неправомерного обращения с техническими средствами негласного получения информации, предложено установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 2 ст. 137 «Нарушение неприкосновенности частной жизни», ч. 2 ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ, ч. 2 ст. 141 «Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий» и ч. 3 ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ;

– доказана целесообразность установления в ст. 226.1 «Контрабанда сильнодействующих, ядовитых, отравляющих, взрывчатых, радиоактивных веществ, радиационных источников, ядерных материалов, огнестрельного оружия или его основных частей, взрывных

устройств, боеприпасов, оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а также материалов и оборудования, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а равно стратегически важных товаров и ресурсов или культурных ценностей либо особо ценных диких животных и водных биологических ресурсов» УК РФ ответственности за контрабанду специальных технических средств, используемых для негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, путем внесения следующих дополнений в наименование ст. 226.1 УК РФ и в диспозицию ч. 1 ст. 226.1 УК РФ: после слов *«ядерных материалов»* указать *«технических средств негласного получения информации, специальных технических средств, предназначенных для нарушения систем защиты цифровой информации»*;

– в целях государственного регулирования правоотношений, возникающих при обороте технических средств негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации и предупреждения соответствующих деяний, аргументировано предложение о принятии отдельного федерального закона «О специальных технических средствах». В нем необходимо определить правила их оборота, содержание используемых понятий, субъекты, которым разрешено использовать указанные средства, установить порядок их применения и т. д.

Более 57 % респондентов согласны с предложением об установлении повышенной уголовной ответственности за применение таких средств в ст. 137 «Нарушение неприкосновенности частной жизни», 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений», 141 «Воспрепятствование осуществлению избирательных прав или работе избирательных

комиссий», 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ и с тезисом о принятии федерального закона «О специальных технических средствах»[436] (см. Приложения 1–3).

3. Поскольку оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, имеет повышенную опасность, предложено:

– установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 3 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ и в ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ;

– ввести отдельную норму об ответственности за незаконные производство, приобретение и (или) сбыт таких средств в следующей авторской редакции:

> *«Статья 273.1. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации*
> *1. Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для нарушения систем защиты цифровой информации,–*
> *наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.*

[436] Бегишев И. Р. Преступления в сфере обращения цифровой информации. Результаты научного исследования // Information Security / Информационная безопасность. 2012. № 6. С. 9.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения,–
наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

4. Предлагается установить уголовную ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем, и дополнить УК РФ ст. 272.1 в следующей редакции:

«Статья 272.1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем
1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем,–
наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.
2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения,–
наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет,

либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

Целесообразность установления уголовной ответственности за приобретение или сбыт цифровой информации, заведомо добытой преступным путем, поддерживают более 85 % респондентов, принявших участие в экспертном опросе[437] (см. Приложения 1–3).

[437] Там же.

ЗАКЛЮЧЕНИЕ

Опасность и обороты преступности в сфере обращения цифровой информации стремительно растут. По прогнозам ведущего мирового исследовательского центра по вопросам кибербезопасности *Cybersecurity Ventures*, мировой оборот киберпреступности достигнет $6 трлн в год к 2021 г. по сравнению с $3 трлн в 2015 г. Ожидается, что через три года киберпреступность будет более прибыльной, чем глобальная торговля всеми основными нелегальными наркотиками, вместе взятыми[438]. Все это вызывает необходимость глубокого и своевременного, в том числе прогностического, научного обеспечения проблемы.

Сформулируем основные выводы проведенного авторами исследования.

С появлением беспроводных систем связи чрезвычайно расширилась и сфера обращения информации. Она теперь повсюду: в компьютерах, телефонах, телевизорах, пылесосах, пространстве и т. д. Поэтому сведение охраняемой информации только к собственно компьютерной, как это делается в гл. 28 «Преступления в сфере компьютерной информации» УК РФ, не вполне корректно. С технической точки зрения в современных информационно-телекоммуникационных системах обращается не компьютерная, а цифровая информация. Первая является лишь подвидом второй. Под цифровой информацией мы предлагаем понимать сведения (сообщения, данные), обращающиеся в информационно-телекоммуникационных устройствах, их системах и сетях. Учитывая, что термин «цифровая информация» является более полным и точным, чем термин «компьютерная информация», рекомендуем именно его

[438] Cybercrime Damages $6 Trillion By 2021 // Cybersecurity Ventures. URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (дата обращения: 23.05.2019).

использовать в соответствующих статьях Особенной части УК РФ и других нормативных актах.

Под преступлением в сфере обращения цифровой информации предлагается понимать предусмотренное уголовным законом виновное совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации. При этом защищаемыми свойствами цифровой информации ограниченного доступа являются ее конфиденциальность, целостность и достоверность, а общедоступной информации – ее целостность, достоверность и доступность.

В целях упорядочения терминологии, обеспечения единства и системности уголовного и иного отраслевого законодательства предложено использовать более широкий по содержанию термин «информационно-телекоммуникационные устройства, их системы и сети» в статьях Особенной части УК РФ вместо предусмотренного в ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ термина, указывающего на объекты обращения цифровой информации в виде «средств хранения, обработки или передачи компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования».

Поскольку сеть Интернет содержит интернет-ресурсы, размещающие информацию о способах совершения преступлений в сфере компьютерной информации, а также объявления о предоставлении незаконных услуг в этой сфере, предлагается в порядке предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «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» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом: «е) информации о способах совершения преступлений в сфере цифровой информации, а также объявлений по предоставлению незаконных услуг в этой сфере».

Все большее распространение принимают компьютерные атаки, под которыми рекомендуем понимать преднамеренные действия в отношении информационной инфраструктуры, повлекшие нарушение достоверности, целостности и конфиденциальности цифровой информации.

Предложено ввести в правовую науку термин «феномен безопасной компьютерной атаки» и определить его как состояние субъектов информационных правоотношений, осознающих опасность нарушения и важность обеспечения безопасности информационной инфраструктуры, но не обеспечивающих ее в силу различных причин, в том числе при проведении в отношении нее компьютерных атак. Установлено, что потеря цифровой информации во многом обусловлена отсутствием у сотрудников организаций знаний базовых основ обеспечения информационной безопасности. Безопасность атаки относится в данном случае к атакующему субъекту. Думается, что данный термин может быть использован в качестве оценочного индикатора в системе обеспечения информационной безопасности субъектов информационных правоотношений.

К причинам феномена безопасной компьютерной атаки можно отнести:

– пренебрежение и халатность;

– нежелание нести финансовые расходы на обеспечение информационной безопасности информационной инфраструктуры;

– несоответствие систем защиты цифровой информации информационных систем и сетей уровню угроз их информационной безопасности;

– низкий уровень культуры информационной безопасности;

– нехватку квалифицированных специалистов по защите информации, в том числе специально-ориентированного профиля.

Поскольку общественная опасность неправомерного доступа к цифровой информации близка по своей сути и общественной опасности перехвату цифровой информации в пространстве и в связи с отсутствием в УК РФ нормы, предусматривающей ответственность за перехват цифровой информации, предлагается включить упоминание о данном деянии в наименование ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ и в диспозицию ч. 1 этой статьи.

Часть 1 ст. 272 УК РФ не регулирует ситуацию, при которой вследствие неправомерного доступа к цифровой информации происходит ознакомление с ней, что исключает ответственность за огромный пласт возможных преступных посягательств. Поэтому предлагаем включить в норму указание на данный способ совершения преступления.

Результаты неправомерного доступа к компьютерной информации не только могут вызвать, например, временные сбои в работе всей информационной системы организации, но и парализовать ее на длительное время, что, на наш взгляд, заслуживает уголовной ответственности. Поэтому в число альтернативных последствий, предусмотренных ч. 1 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ, следует включить «нарушение работы информационно-телекоммуникационных устройств, их систем и сетей».

В результате название и ч. 1 ст. 272 УК РФ примут следующий вид:

«Статья 272. Неправомерный доступ к охраняемой законом цифровой информации или ее перехват

1. Неправомерный доступ к охраняемой законом цифровой информации, а равно незаконный ее перехват, если это деяние повлекло уничтожение, блокирование, модификацию, копирова-

ние цифровой информации, ознакомление с ней либо нарушение работы информационно-телекоммуникационных устройств, их систем и сетей,–

наказывается…» (далее по тексту УК РФ).

В примечании 3 к ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ предлагаем дать следующее определение понятия: «Под перехватом цифровой информации понимается процесс неправомерного ее получения в пространстве».

Установление крупного ущерба для преступлений, предусмотренных гл. 28 «Преступления в сфере компьютерной информации» УК РФ, в размере свыше одного миллиона рублей представляется нам неоправданным. Ущерб в несколько десятков или сотен тысяч рублей для граждан или субъектов малого бизнеса вполне может иметь для них фатальные последствия. Размер в сто тысяч, на наш взгляд, тоже заслуживает отнесения к крупному.

Кроме того, предлагаем включить в ст. 272 УК РФ дополнительные квалифицирующие признаки, такие как совершение деяния из хулиганских побуждений, с использованием специальных технических средств, предназначенных для нарушения систем защиты цифровой информации.

В ч. 4 ст. 272 УК РФ установлена ответственность за деяния, предусмотренные предыдущими частями этой статьи, если они повлекли тяжкие последствия или создали угрозу их наступления. Хотелось бы, чтобы законодатель в примечании к статье перечислил хотя бы примерный перечень таких последствий, что существенно облегчило бы работу правоприменителя. Безусловно, сюда должны относиться такие последствия, как причинение смерти либо тяжкого вреда здоровью по неосторожности. Аналогичные пожелания законодателю адресуем и применительно к ч. 4 ст. 273 УК РФ, в которой также указаны тяжкие последствия.

Законодатель в ч. 1 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ установил

в числе прочего ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для нейтрализации средств защиты компьютерной информации. Нам представляется, что использование слова «нейтрализация» в данном случае не совсем уместно, поскольку оно не является устоявшимся понятием в русском языке и не имеет единого смыслового значения. Считаем, что более удачным решением была бы замена термина «нейтрализация» на термин «нарушение», который широко используется в российском уголовном законе.

Предложено также уточнение использованного в ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ термина, указывающего на объекты обращения цифровой информации. В результате обоснована рекомендация об изложении наименования ст. 274 УК РФ и диспозиции ч. 1 этой статьи в следующей редакции:

«Статья 274. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей

1. Нарушение правил эксплуатации или иное нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом цифровой информации, причинившее крупный ущерб,–

наказывается…» (далее по тексту УК РФ)

Поскольку деяния, предусмотренные ст. 272, 273, 274, 274.1 УК РФ, представляют собой единую систему преступлений, посягающих на цифровую информацию, предлагается гл. 28 УК РФ назвать «Преступления в сфере обращения цифровой информации», а ст. 272 и 273 УК РФ озаглавить как «Неправомерный доступ к цифровой информации или ее перехват» и «Создание, использование и распространение вредоносных цифровых программ» соответственно.

Понятие «безопасность критической информационной инфраструктуры» является видовым по отношению к понятию «информационная безопасность», которое, в свою очередь, входит в объем понятия «национальная безопасность». Поэтому обеспечение безопасности критической информационной инфраструктуры должно основываться на принципах и методологии обеспечения национальной безопасности.

Законодатель почему-то не отнес к субъектам критической информационной инфраструктуры участников таких видов экономической деятельности, как жилищно-коммунальное хозяйство, строительство, сельское хозяйство, пищевая промышленность и ряд других. Это обстоятельство нуждается, на наш взгляд, в исправлении. Поскольку, например, нарушение в результате компьютерной атаки функционирования государственной информационной системы жилищно-коммунального хозяйства, одной из важнейших социально значимых информационных систем государства, чревато очень серьезными последствиями. По нашему мнению, для успешного решения этого вопроса необходимо использовать данные Общероссийского классификатора видов экономической деятельности (ОКВЭД 2). Именно по его данным следует соотносить вид экономической деятельности с предполагаемым субъектом критической информационной инфраструктуры.

Безопасность критической информационной инфраструктуры зависит не только от степени государственного контроля в этой сфере, но и от выполнения субъектами критической информационной инфраструктуры (бизнес-сообществом) конкретных требований по созданию систем безопасности и обеспечению их функционирования. Это важнейший вопрос самосохранения бизнеса.

Статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» УК РФ представляет собой структуру, являющуюся своего рода надстройкой (специальной нормой) над тремя преступлениями в сфере

компьютерной информации: ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ; ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ; ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» УК РФ. Это обстоятельство создает несколько проблем, что требует совершенствования норм уголовного законодательства.

Обосновано и предложено создание Федеральной службы информационной безопасности Российской Федерации – отечественного единого специального федерального органа исполнительной власти в сфере расследования и предупреждения преступлений в цифровой сфере, включая уголовно-правовое обеспечение безопасности объектов критической информационной инфраструктуры, а также воздействие на информационные инфраструктуры противника.

Кроме того, предлагаем разработать и внедрить следующие инструменты:

– *ФГОС ВО по направлению «Безопасность критической информационной инфраструктуры»;*

– *курсы переподготовки и повышения квалификации по направлению «Безопасность критической информационной инфраструктуры»;*

– *механизм повышения квалификации должностных лиц субъектов критической информационной инфраструктуры по различным вопросам обеспечения ее безопасности;*

– *механизм страхового обеспечения безопасности критической информационной инфраструктуры;*

– *механизм организации всероссийских, региональных и отраслевых киберучений на объектах критической информационной инфраструктуры Российской Федерации.*

Крайне опасным является мошенническое программное обеспечение, позволяющее нарушать системы защиты цифровой

информации. Сегодня зачастую такое программное обеспечение, к сожалению, находится в свободном доступе в информационно-телекоммуникационной сети Интернет или же нелегально приобретается на соответствующих виртуальных площадках у их разработчиков. Поэтому предлагаем включить в «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», сайты, содержащие или распространяющие вредоносные компьютерные программы, мошенническое программное обеспечение и программные средства, предназначенные для нарушения систем защиты информации информационно-телекоммуникационных устройств, их систем и сетей.

Поскольку деяние, предусмотренное ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ, относится к преступлениям в сфере обращения цифровой информации и совершается с ее использованием, то указанную статью предлагается назвать «Мошенничество с использованием цифровой информации».

Доказано, что мошенническое программное обеспечение относится к категории вредоносных цифровых программ. Уголовная ответственность за создание, использование и распространение мошеннического программного обеспечения (мошеннических программ) должна наступать по ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ.

С целью дифференциации ответственности за мошенничество в сфере цифровой информации предлагается внести в ч. 2 ст. 159.6 «Мошенничество в сфере компьютерной информации» УК РФ следующий квалифицирующий признак: после слов *«значительного ущерба гражданину»* указать *«или с нарушением системы защиты цифровой информации».*

Поскольку информационно-телекоммуникационная сеть Интернет содержит интернет-ресурсы, размещающие информацию

о вредоносных компьютерных программах и программных средствах, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей, предлагается в целях предупреждения этих преступлений ввести механизм внесудебного ограничения доступа на территории Российской Федерации к такой информации, дополнив п. 1 ч. 5 ст. 15.1 «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» Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» следующим пунктом:

«ж) вредоносных программ и программных средств, предназначенных для нарушения систем защиты цифровой информации информационно-телекоммуникационных устройств, их систем и сетей».

Предлагается вместо вызывающего неоднозначные трактовки термина «специальные технические средства, предназначенные для негласного получения информации» использовать в УК РФ более точный и недвусмысленный термин «технические средства негласного получения информации». При этом в примечании к ст. 138.1 «Незаконный оборот специальных технических средств, предназначенных для негласного получения информации» УК РФ рекомендовано изложить соответствующее определение понятия в следующей редакции: «Под техническим средством негласного получения информации следует понимать программное либо аппаратное устройство, созданное или приспособленное для негласного перехвата, обработки и анализа информации».

Поскольку в УК РФ недостаточно учтена общественная опасность неправомерного обращения с техническими средствами негласного получения информации, предложено установить в качестве

квалифицирующего признака ответственность за применение таких средств в ч. 2 ст. 137 «Нарушение неприкосновенности частной жизни», ч. 2 ст. 138 «Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений» УК РФ, ч. 2 ст. 141 «Воспрепятствование осуществлению избирательных прав или работе избирательных комиссий» и ч. 3 ст. 183 «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну» УК РФ.

Авторами также доказана целесообразность установления в ст. 226.1 «Контрабанда сильнодействующих, ядовитых, отравляющих, взрывчатых, радиоактивных веществ, радиационных источников, ядерных материалов, огнестрельного оружия или его основных частей, взрывных устройств, боеприпасов, оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а также материалов и оборудования, которые могут быть использованы при создании оружия массового поражения, средств его доставки, иного вооружения, иной военной техники, а равно стратегически важных товаров и ресурсов или культурных ценностей либо особо ценных диких животных и водных биологических ресурсов» УК РФ ответственности за контрабанду специальных технических средств, используемых для негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, путем внесения следующих дополнений в наименование ст. 226.1 УК РФ и в диспозицию ч. 1 ст. 226.1 УК РФ: после слов *«ядерных материалов»* указать *«технических средств негласного получения информации, специальных технических средств, предназначенных для нарушения систем защиты цифровой информации»*.

В целях государственного регулирования правоотношений, возникающих при обороте технических средств негласного получения информации, а также специальных технических средств, предназначенных для нарушения систем защиты цифровой информации

и предупреждения соответствующих деяний, аргументировано предложение о принятии отдельного федерального закона «О специальных технических средствах». В нем необходимо определить правила их оборота, содержание используемых понятий, субъекты, которым разрешено использовать указанные средства, установить порядок их применения и т. д.

Необходима криминализация оборота специальных технических средств, предназначенных для нарушения систем защиты цифровой информации и проникновения в информационно-телекоммуникационные устройства, системы и их сети, ввиду их повышенной опасности в качестве орудий и средств совершения преступлений. В этой связи предлагается установить в качестве квалифицирующего признака ответственность за применение таких средств в ч. 3 ст. 272 «Неправомерный доступ к компьютерной информации» УК РФ и в ч. 2 ст. 273 «Создание, использование и распространение вредоносных компьютерных программ» УК РФ. А также ввести отдельную норму об ответственности за незаконные производство, приобретение и (или) сбыт таких средств в следующей авторской редакции:

«Статья 273.1. Незаконный оборот специальных технических средств, предназначенных для нарушения систем защиты цифровой информации

1. Незаконные производство, приобретение и (или) сбыт специальных технических средств, предназначенных для нарушения систем защиты цифровой информации, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения,–

наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

Учитывая, что ст. 175 «Приобретение или сбыт имущества, заведомо добытого преступным путем» УК РФ не содержит указаний на такой предмет, как цифровая информация, предлагается установить уголовную ответственность за приобретение или сбыт цифровой информации, заведомо добытой преступным путем, и дополнить УК РФ ст. 272.1 в следующей редакции:

«Статья 272.1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем

1. Приобретение или сбыт охраняемой законом цифровой информации, заведомо добытой преступным путем,–

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до одного года, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, совершенное группой лиц по предварительному сговору или организованной группой, либо лицом с использованием своего служебного положения,–

наказывается штрафом в размере от двухсот тысяч до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо

исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок».

Данная мера будет направлена в том числе против лиц, которые продают незаконно полученную информацию. На продажу периодически выставляются клиентские базы банков, иных компаний, другие материалы, открытый оборот которых опасен. Некоторые из таких акций серьезно будоражат общественность.

Завершая эту книгу, авторы не прекращают совместные исследования. И готовы к диалогу со всеми, кто интересуется вопросами цифровой преступности и противодействия ей.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

Законодательные, нормативные и иные официальные документы

1. Конституция Российской Федерации: (в редакции Закона Российской Федерации о поправке к Конституции Российской Федерации от 21 июля 2014 г. № 11-ФКЗ) // Российская газета. – 1993. – № 237; Собрание законодательства Российской Федерации. – 2014. – № 31. – Ст. 4398.

2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 25. – Ст. 2954.

3. Уголовный процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 52 (ч. I). – Ст. 4921.

4. Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 1 (часть I). – Ст. 1.

5. О внесении изменения в статью 138.1 Уголовного кодекса Российской Федерации: Федеральный закон № 308-ФЗ от 2 августа 2019 г. // Собрание законодательства Российской Федерации. – 2019. – № 31. – Ст. 4467.

6. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон № 187-ФЗ от 26 июля 2017 г. // Собрание законодательства Российской Федерации. – 2017. – № 31 (ч. I). – Ст. 4736.

7. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон № 207-ФЗ от 29 ноября 2012 г. // Собрание законодательства Российской Федерации. – 2012. – № 49. – Ст. 6752.

8. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «Об информации, информационных технологиях и о защите информации»: Федеральный закон № 200-ФЗ от 11 июля 2011 г. // Собрание законодательства Российской Федерации. – 2011. – № 29. – Ст. 4291.

9. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный

закон № 420-ФЗ от 7 декабря 2011 г. // Собрание законодательства Российской Федерации. – 2011. – № 50. – Ст. 7362.

10. О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства: Федеральный закон № 57-ФЗ от 29 апреля 2008 г. // Собрание законодательства Российской Федерации. – 2008. – № 18. – Ст. 1940.

11. О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием государственного контроля в сфере частной охранной и детективной деятельности: Федеральный закон № 272-ФЗ от 22 декабря 2008 г. // Собрание законодательства Российской Федерации. – 2008. – № 52 (ч. I). – Ст. 6227.

12. О противодействии терроризму: Федеральный закон № 35-ФЗ от 6 марта 2006 г. // Собрание законодательства Российской Федерации. – 2006. – № 11. – Ст. 1146.

13. Об информации, информационных технологиях и о защите информации: Федеральный закон № 149-ФЗ от 27 июля 2006 г. // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. I). – Ст. 3448.

14. О персональных данных: Федеральный закон № 152-ФЗ от 27 июля 2006 г. // Собрание законодательства Российской Федерации. – 2006. – № 31 (ч. I). – Ст. 3451.

15. О связи: Федеральный закон № 126-ФЗ от 7 июля 2003 г. // Собрание законодательства Российской Федерации. – 2003. – № 28. – Ст. 2895.

16. Об оперативно-розыскной деятельности: Федеральный закон № 144-ФЗ от 12 августа 1995 г. // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

17. Об особенностях обеспечения информационной безопасности критически важных объектов информационной и телекоммуникационной инфраструктуры: Законопроект № 340741–4 // Автоматизированная система обеспечения законодательной деятельности Государственной Думы Российской Федерации. – URL: http://asozd2.duma.gov.ru/main.nsf/(Spravka)? OpenAgent&RN=340741–4&11 (дата обращения: 23.05.2019).

18. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года: Указ Президента Российской Федерации № 204 от 7 мая 2018 г. // Собрание законодательства Российской Федерации. – 2018. – № 20. – Ст. 2817.

19. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента Российской Федерации № 351 от 17 марта 2008 г. // Собрание законодательства Российской Федерации. – 2008. – № 12. – Ст. 1110.

20. О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации: Указ Президента Российской Федерации № 31с от 15 января 2013 г. // Собрание законодательства Российской Федерации. – 2013. – № 3. – Ст. 178.

21. О внесении изменений в Положение о Федеральной службе охраны Российской Федерации, утвержденное Указом Президента Российской Федерации № 1013 от 7 августа 2004 г.: Указ Президента Российской Федерации № 89 от 27 февраля 2018 г. // Собрание законодательства Российской Федерации. – 2018. – № 10. – Ст. 1477.

22. О некоторых вопросах информационной безопасности Российской Федерации: Указ Президента Российской Федерации № 260 от 22 мая 2015 г. // Собрание законодательства Российской Федерации. – 2015. – № 21. – Ст. 3092.

23. О Стратегии национальной безопасности Российской Федерации: Указ Президента Российской Федерации № 683 от 31 декабря 2015 г. // Собрание законодательства Российской Федерации. – 2016. – № 1 (ч. II). – Ст. 212.

24. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента Российской Федерации № 646 от 5 декабря 2016 г. // Собрание законодательства Российской Федерации. – 2016. – № 50. – Ст. 7074.

25. Концепция противодействия терроризму в Российской Федерации: утверждена Президентом Российской Федерации 5 октября 2009 г. // Российская газета. – 2009. – № 198.

26. Об утверждении Положения о лицензировании деятельности физических и юридических лиц, не уполномоченных на осуществление оперативно-розыскной деятельности, связанной с разработкой, производством, реализацией, приобретением в целях продажи, ввоза в Российскую Федерацию и вывоза за ее пределы специальных технических средств, предназначенных (разработанных, приспособленных, запрограмми-

рованных) для негласного получения информации, и перечня видов специальных технических средств, предназначенных (разработанных, приспособленных, запрограммированных) для негласного получения информации в процессе осуществления оперативно-розыскной деятельности: Постановление Правительства Российской Федерации № 770 от 1 июля 1996 г. // Собрание законодательства Российской Федерации. – 1996. – № 28. – Ст. 3382.

27. Об утверждении Положения о ввозе в Российскую Федерацию и вывозе из Российской Федерации специальных технических средств, предназначенных для негласного получения информации, и списка видов специальных технических средств, предназначенных для негласного получения информации, ввоз и вывоз которых подлежат лицензированию: Постановление Правительства Российской Федерации № 214 от 10 марта 2000 г. // Собрание законодательства Российской Федерации. – 2000. – № 12. – Ст. 1292.

28. Об утверждении Положения о лицензировании деятельности по разработке, производству, реализации и приобретению в целях продажи специальных технических средств, предназначенных для негласного получения информации: Постановление Правительства Российской Федерации № 287 от 12 апреля 2012 г. // Собрание законодательства Российской Федерации. – 2012. – № 16. – Ст. 1885.

29. Об утверждении Положения о лицензировании деятельности по выявлению электронных устройств, предназначенных для негласного получения информации (за исключением случая, если указанная деятельность осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя): Постановление Правительства Российской Федерации № 314 от 16 апреля 2012 г. // Собрание законодательства Российской Федерации. – 2012. – № 17. – Ст. 1988.

30. О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено»: Постановление Правительства Российской Федерации № 1101 от 26 октября 2012 г. // Собрание законодательства Российской Федерации. – 2012. – № 44. – Ст. 6044.

31. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства Российской Федерации № 127 от 8 февраля 2018 г. // Собрание законодательства Российской Федерации. – 2018. – № 8. – Ст. 1204.

32. Об одобрении Концепция федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры Российской Федерации и опасных грузов: Распоряжение Правительства Российской Федерации № 1314-р от 27 августа 2005 г. // Собрание законодательства Российской Федерации. – 2005. – № 35. – Ст. 3660.

33. О проекте федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона “Об информации, информационных технологиях и о защите информации”»: Распоряжение Правительства Российской Федерации № 1097-р от 30 июня 2010 г. // Собрание законодательства Российской Федерации. – 2010. – № 27. – Ст. 3544.

34. Руководящий документ Гостехкомиссии России «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации». – М.: ГТК РФ, 1992. – 6 с.

35. ГОСТ Р 50922–2006. «Защита информации. Основные термины и определения». – М.: Стандартинформ, 2008. – 12 с.

36. ГОСТ Р 51275–2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». – М.: Стандартинформ, 2007: утвержден и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. № 374-ст «Об утверждении национального стандарта». Текст приказа официально опубликован не был. – 11 с.

37. Конвенция о компьютерных преступлениях от 23 ноября 2001 г. (ETS № 185) // Совет Европы. Бюро договоров. – URL: http://www.coe.int/it/web/conventions/home/-/conventions/rms/0900001680081580 (дата обращения: 23.05.2019).

38. Уголовный кодекс Украины. – URL: http://kodeksy.com.ua/ka/ugolovnyj_kodeks_ukraini.htm (дата обращения: 23.05.2019).

39. Уголовный кодекс Республики Узбекистан. – URL: http://fmc.uz/legisl.php?id=k_ug (дата обращения: 23.05.2019).

40. Уголовный кодекс Французской Республики. – URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата обращения: 23.05.2019).

41. О мерах нетарифного регулирования: Решение Коллегии Евразийской экономической комиссии № 30 от 21 апреля 2015 г. // Правовой портал Евразийского экономического союза, 22 апреля 2015 г. – URL: https://docs.eaeunion.org (дата обращения: 23.05.2019).

42. Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды: Приказ Федеральной службы по техническому и экспортному контролю № 31 от 14 марта 2014 г. // Российская газета. – 2014. – № 175.

43. О вводе в эксплуатацию государственной информационной системы жилищно-коммунального хозяйства: Приказ Министерства связи и массовых коммуникаций Российской Федерации № 264 от 14 июня 2016 г. // Официальный сайт Министерства связи и массовых коммуникаций Российской Федерации. – URL: http://minsvyaz.ru/ru/documents/5069/ (дата обращения: 15.05.2017).

44. О принятии и введении в действие Общероссийского классификатора видов экономической деятельности (ОКВЭД2) ОК 029–2014 (КДЕС Ред. 2) и Общероссийского классификатора продукции по видам экономической деятельности (ОКПД2) ОК 034–2014 (КПЕС 2008): Приказ Федерального агентства по техническому регулированию и метрологии № 14-ст от 31 января 2014 г. // Бухгалтерское приложение к газете «Экономика и жизнь». – 2014. – № 21.

45. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: Приказ Федеральной службы по техническому и экспортному контролю № 235 от 21 декабря 2017 г. // Официальный интернет-портал правовой информации, 22 февраля 2018 г. – URL: www.pravo.gov.ru (дата обращения: 23.05.2019).

46. Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ Федеральной службы по техническому и экспортному контролю № 227 от 6 декабря 2017 г. // Официальный интернет-портал правовой информации, 9 февраля 2018 г. – URL: www.pravo.gov.ru (дата обращения: 23.05.19).

Научные статьи, сборники научных трудов, другие публикации

47. Albrecht, D. Chinese Cybersecurity Law Compared to EUNIS-Directive and German IT-Security Act. When cybersecurity not only protects interests of the masses but ultimately also safeguards national sovereignty / D. Albrecht // Recherchieren unter juris (Das Rechtsportal). – 2018. – P. 1–5.

48. August, T., August, R., Shin, H. Designing user incentives for cybersecurity / T. August, R. August, H. Shin // Communications of the ACM. – 2014. – № 57 (11). – P. 43–46.

49. Bajramovic, E. Cyber security in private industry critical infrastructure / E. Bajramovic // International Journal of Economics and Law. – 2015. – № 13 (5). – P. 9–15.

50. Begishev, I. R. Information infrastructure of safe computer attack / I. R. Begishev, Z. I. Khisamova, G. I. Mazitova // Helix. – 2019. – V. 9, № 5. – P. 5639–5642.

51. Begishev, I. R. Criminal legal ensuring of security of critical information infrastructure of the Russian Federation / I. R. Begishev, Z. I. Khisamova, G. I. Mazitova // Revista Gênero & Direito. – 2019. – V. 8, № 6. – P. 283–292.

52. Bikeev, I. I. Experience of Civil Government of Russian Federation Subjects with Institutions of Civil Society in the Sphere of Corruption / I. I. Bikeev, S. G. Nikitin, Z. I. Khisamova, I. R. Begishev, A. Y. Bokovnya // International Journal of Innovative Technology and Exploring Engineering. – 2019. – V. 9, № 1. – P. 5184–5187.

53. Bikeev, I. I. Criminological Risks and Legal Aspects of Artificial Intelligence Implementation / I. I. Bikeev, P. A. Kabanov, I. R. Begishev, Z. I. Khisamova // ACM International Conference on Artificial Intelligence, Information Processing and Cloud Computing (AIIPCC2019). – 2019. – December 2019, Sanya, China.

54. Bokovnya, A.Y. Study of Russia and the UK legislations in combating digital crimes / A.Y. Bokovnya, Z.I. Khisamova, I.R. Begishev // Helix. – 2019. – V. 9, № . 5. – P. 5458–5461.

55. Bovis, C.H. Risk in public-private partnerships and critical infrastructure / C.H. Bovis // European Journal of Risk Regulation. – 2015. – № 6 (2). – P. 200–207.

56. Brem, S. Critical Infrastructure Protection from a National Perspective / S. Brem // European Journal of Risk Regulation. – 2015. – № 6 (2). – P. 191–199.

57. Carr, M. Public–private partnerships in national cyber-security strategies / M. Carr // International Affairs. – 2016. – № 92 (1). – P. 43–62.

58. Coman, I.M. Cross-Border Cyber-Attacks and Critical Infrastructure Protection / I.M. Coman // International Journal of Information Security and Cybercrime. – 2017. – № 2 (6). – P. 47–52.

59. Cohen-Almagor, R. Internet architecture, freedom of expression and social responsibility: Critical realism and proposals for a better future / R. Cohen-Almagor // Innovation: The European Journal of Social Science Research. – 2015. – № 28 (2). – P. 147–166.

60. Dunn-Cavelty, M. Public–private partnerships are no silver bullet: An expanded governance model for critical infrastructure protection / M. Dunn-Cavelty, M. Suter // International Journal of Critical Infrastructure Protection. – 2009. – № 2 (4). – P. 179–187.

61. Hathaway, O. A. The Law of Cyber-Attack / O.A. Hathaway, R. Crootof, P. Levitz, H. Nix // California Law Review. – 2012. – № 100. – P. 817–886.

62. Khisamova, Z. I. On Methods to Legal Regulation of Artificial Intelligence in the World / Z. I. Khisamova, I. R. Begishev, R. R. Gaifutdinov // International Journal of Innovative Technology and Exploring Engineering. – 2019. – V. 9, № 1. – P. 5159–5162.

63. Min, K.-S., Chai, S.-W., Han, M. An international comparative study on cyber security strategy / K.-S. Min, S.-W. Chai, M. Han // International Journal of Security and Its Applications. – 2015. – № 9 (2). – P. 13–20.

64. Orji, U.J. Towards the Regional Harmonization of E-Commerce Regulation in Africa A Comparative Analysis of the African Union's E-Commerce Regime / U.J. Orji // Recherchieren unter juris (Das Rechtsportal). – 2018. – P. 12–22.

65. Shackelford, S. J. From Russia with Love: Understanding the Russian Cyber Threat to U. S. Critical Infrastructure and What to Do about It / S. J. Shackelford, M. Sulmeyer, A. N. Craig Deckard, B. Buchanan, B. Micic // Nebraska Law Review. – 2017. – № 96. – P. 320–338.

66. Venkatachary, S. K. Economic Impacts of Cyber Security in Energy Sector: A Review / S. K. Venkatachary, J. Prasad, R. Samikannu // International Journal of Energy Economics and Policy. – 2017. – № 7 (5). – P. 250–262.

67. Walker, C., Conway, M. Online terrorism and online laws / C. Walker, M. Conway // Dynamics of Asymmetric Conflict. – 2015. – № 8 (2). – P. 156–175.

68. Wiater, P. On the notion of «partnership» in critical infrastructure protection / P. Wiater // European Journal of Risk Regulation. – 2015. – № 6 (2). – P. 255–262.

69. The ITU publication Understanding cybercrime: phenomena, challenges and legal response has been prepared by Prof. Dr. Marco Gercke and is a new edition of a report previously entitled Understanding Cybercrime: A Guide for Developing Countries. The author wishes to thank the Infrastructure Enabling Environment and E-Application Department, ITU Telecommunication Development Bureau. – URL: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/legislation.aspx (дата обращения: 23.05.2019).

70. 10 тезисов интернет-безопасности // Information Security / Информационная безопасность. – 2011. – № 6. – С. 22–23.

71. Агапов, П. В. Международно-правовые основы обеспечения информационной безопасности участников содружества независимых государств / П. В. Агапов, М. А. Ефремова // Юридическая наука и правоохранительная практика. – 2015. – № 1. – С. 176–182.

72. Александрова, Н. С. Преступления в сфере компьютерной информации в российском уголовном праве / Н. С. Александрова // Вестник Димитровградского инженерно-технологического института. – 2015. – № 3. – С. 114–119.

73. Анапольская, А. И. Снятие информации с технических каналов связи: условия гарантирования прав и свобод человека и гражданина / А. И. Анапольская, В. Н. Влазнев // Вопросы современной науки и практики. Университет им. В. И. Вернадского. – 2015. – № 2. – С. 96–100.

74. Антонов, О. Ю. Анализ преступной деятельности, совершаемой с использованием информационно-телекоммуникационных сетей /

О. Ю. Антонов // Вестник Академии Следственного комитета Российской Федерации. – 2017. – № 4 (14). – С. 132–138.

75. Антонов, О. Ю. Выявление дополнительных эпизодов и новых видов порно-сексуальной преступной деятельности, совершаемой с использованием информационно-телекоммуникационных сетей / О. Ю. Антонов // Расследование преступлений: проблемы и пути их решения. – 2017. – № 3 (17). – С. 169–177.

76. Антопольский, А. Б. Государственный надзор и охрана прав владельцев цифровых объектов / А. Б. Антопольский // Сборник тезисов докладов участников десятой Всероссийской конференции «Проблемы законодательства в сфере информатизации». – М.: Изд-во «ВНИИПВТИ», 2002. – С. 20–24.

77. Арзамасцев, М. В. К вопросу об уголовно-правовой классификации киберпреступлений / М. В. Арзамасцев // Актуальные вопросы права и отраслевых наук. – 2017. – № 1 (3). – С. 11–16.

78. Бабушкин, Г. Д., Филиппенко, В. И. Юридическая психология как научная дисциплина / Г. Д. Бабушкин, В. И. Филиппенко // Психопедагогика в правоохранительных органах. – 1997. – № 2. – С. 114–118.

79. Барташевич, С. А. Информационная безопасность – залог успеха бизнеса / С. А. Барташевич // Information Security / Информационная безопасность. – 2017. – № 4. – С. 19.

80. Бегишев, И. Р. Безопасность критической информационной инфраструктуры Российской Федерации / И. Р. Бегишев // Безопасность бизнеса. – 2019. – № 1. – С. 27–32.

81. Бегишев, И. Р. Синдром безопасной атаки: юридико-психологический феномен / И. Р. Бегишев // Юридическая психология. – 2018. – № 2. – С. 27–30.

82. Бегишев, И. Р. Криминологические риски применения искусственного интеллекта / И. Р. Бегишев, З. И. Хисамова // Всероссийский криминологический журнал. – 2018. – Т. 12, № 6. – С. 767–775.

83. Бегишев, И. Р. Федеральная служба информационной безопасности Российской Федерации: миф или реальность? / И. Р. Бегишев // Information Security / Информационная безопасность. – 2016. – № 6. – С. 14–15.

84. Бегишев, И. Р. Изготовление, сбыт и приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации: правовой аспект / И. Р. Бегишев // Информация и безопасность. – 2010. – № 2. – С. 255–258.

85. Бегишев, И. Р. Информационное оружие как средство совершения преступлений / И. Р. Бегишев // Информационное право. – 2010. – № 4. – С. 23–25.

86. Бегишев, И. Р. Информационные войны: предупреждение и предотвращение угроз / И. Р. Бегишев // Защита информации. Inside. – 2010. – № 4. – С. 34–35.

87. Бегишев, И. Р. Меры предупреждения преступлений в сфере обращения цифровой информации / И. Р. Бегишев // Информация и безопасность. – 2011. – № 3. – С. 433–438.

88. Бегишев, И. Р. Новое в ответственности за неправомерный доступ к компьютерной информации по Уголовному кодексу Российской Федерации / И. Р. Бегишев // Правосудие в Татарстане. – 2011. – № 4. – С. 42–44.

89. Бегишев, И. Р. Ответственность за нарушение работы информационно–телекоммуникационных устройств, их систем и сетей / И. Р. Бегишев // Безопасность информационных технологий. – 2011. – № 1. – С. 73–75.

90. Бегишев, И. Р. Открытое ПО: вопросы права, безопасности и последствий / И. Р. Бегишев // Information Security / Информационная безопасность. – 2011. – № 4. – С. 28–29.

91. Бегишев, И. Р. Перехват охраняемой законом цифровой информации: уголовно–правовые аспекты / И. Р. Бегишев // Информационная безопасность регионов. – 2011. – № 1. – С. 78–81.

92. Бегишев, И. Р. Правовые аспекты безопасности информационного общества / И. Р. Бегишев // Информационное общество. – 2011. – № 4. – С. 54–59.

93. Бегишев, И. Р. Преступления в сфере обращения цифровой информации. Результаты научного исследования / И. Р. Бегишев // Information Security / Информационная безопасность. – 2012. – № 6. – С. 8–10.

94. Бегишев, И. Р. Преступления в сфере цифровой информации: состояние, пробелы и пути их решения / И. Р. Бегишев // Информационное право. – 2010. – № 2. – С. 18–21.

95. Бегишев, И. Р. Проблемы противодействия преступным посягательствам на информационные системы критически важных и потенциально опасных объектов / И. Р. Бегишев // Информационная безопасность регионов. – 2010. – № 1. – С. 9–13.

96. Бегишев, И. Р. Противодействие утечкам цифровой информации: вопросы уголовной ответственности / И. Р. Бегишев // Защита информации. Inside. – 2011. – № 2. – С. 32–34.

97. Бегишев, И. Р. Создание, использование и распространение вредоносных компьютерных программ / И. Р. Бегишев // Проблемы права. – 2012. – № 3. – С. 218–221.

98. Бегишев, И. Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем / И. Р. Бегишев // Актуальные проблемы экономики и права. – 2010. – № 1. – С. 123–126.

99. Бегишев, И. Р. Проблемы уголовной ответственности за обращение со специальными техническими средствами, предназначенными для негласного получения информации / И. Р. Бегишев // Следователь. – 2010. – № 5. – С. 2–4.

100. Бегишев, И. Р. Уголовно–правовые аспекты кибертерроризма / И. Р. Бегишев // Правовые вопросы национальной безопасности. – 2010. – № 5–6. – С. 34–37.

101. Бегишев, И. Р. Цифровая информация: понятие и сущность как предмета преступления по российскому уголовному праву / И. Р. Бегишев // Академический юридический журнал. – 2011. – № 2. – С. 47–55.

102. Бегишев, И. Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей / И. Р. Бегишев // Вестник УрФО. Безопасность в информационной сфере. – 2012. – № 1. – С. 15–18.

103. Бегишев, И. Р. Некоторые вопросы противодействия мошенничеству в сфере компьютерной информации / И. Р. Бегишев // Вестник Казанского юридического института МВД России. – 2016. – № 3. – С. 112–117.

104. Бегишев, И. Р. Проблемы ответственности за незаконные действия с информацией, заведомо добытой преступным путем / И. Р. Бегишев // Безопасность информационных технологий. – 2010. – № 1. – С. 43–44.

105. Бегишев, И. Р. Уголовная ответственность за перехват цифровой информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2010. – № 4. – С. 16–17.

106. Бегишев, И. Р. Уголовная ответственность за нарушение работы цифровых устройств, их систем и сетей / И. Р. Бегишев // Information Security / Информационная безопасность. – 2010. – № 5. – С. 22–23.

107. Бегишев, И. Р. Некоторые механизмы совершенствования уголовного законодательства за совершение преступлений в сфере обращения

цифровой информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2017. – № 6. – С. 40–43.

108. Бегишев, И. Р. Уголовно-правовое нововведение в сфере защиты цифровой информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2011. – № 1. – С. 18–19.

109. Бегишев, И. Р. Новеллы в уголовном законодательстве об ответственности за преступления в сфере компьютерной информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2012. – № 2. – С. 52–53.

110. Бегишев, И. Р. Новый взгляд на мошенничество в сфере компьютерной информации / И. Р. Бегишев // Information Security / Информационная безопасность. – 2016. – № 1. – С. 28–29.

111. Бегишев, И. Р. Некоторые аспекты информационной безопасности технологии блокчейн / А. К. Арюков, И. Р. Бегишев, Н. А. Мальцев // Information Security / Информационная безопасность. – 2018. – № 6. – С. 18–19.

112. Бегишев, И. Р. О некоторых способах совершения противоправных деяний в современных информационно-телекоммуникационных системах обращения цифровой информации / И. Р. Бегишев // Информация и безопасность. – 2009. – № 4. – С. 607–610.

113. Бегишев, И. Р Современное состояние преступлений в сфере обращения цифровой информации / И. Р. Бегишев // Информация и безопасность. – 2010. – № 4. – С. 567–572.

114. Бегишев, И. Р Сравнительно-правовой анализ законодательства Великобритании и России в области противодействия преступлениям в цифровой сфере / И. Р. Бегишев, З. И. Хисамова // Baikal Research Journal. – 2019. – Т. 10. – № 3.

115. Бегишев, И. Р Компьютерные атаки на КИИ России: правовые меры защиты / И. Р. Бегишев // Information Security / Информационная безопасность. – 2019. – № 5. – С. 8–10.

116. Бегишев, И. Р. О понятии «электронного средства платежа» в контексте нормы об ответственности за мошенничество, совершенное с его использованием / И. Р. Бегишев // Уголовная политика и культура противодействия преступности: материалы Междунар. науч.-практ. конф., 21 сентября 2018 г.: в 2 т. / редкол.: А. Л. Осипенко, К. В. Вишневецкий, И. А. Паршина, В. С. Соловьев, П. В. Максимов, А. З. Хун. – Краснодар: Краснодарский университет МВД России, 2018. – Т. I. – С. 176–179.

117. Белоножкин, В. И. Информационная сущность и структура терроризма / В. И. Белоножкин // Информация и безопасность. – 2007. – № 4. – С. 541–546.

118. Белоус, В. Г. Проблема квалификации хищений с использованием компьютерных технологий / В. Г. Белоус, Н. С. Градицкая // Актуальные вопросы образования и науки. – 2016. – № 1–2. – С. 49–54.

119. Богданова, Т. Н. К вопросу об определении понятия «преступления в сфере компьютерной информации» / Т. Н. Богданова // Вестник Челябинского государственного университета. – 2012. – № 37. – С. 64–67.

120. Борисов, С. В. К вопросу о противодействии кибертерроризму и киберэкстремизму / С. В. Борисов, А. С. Васнецова, А. Г. Жафяров // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2015. – № 1. – С. 49–55.

121. Боршевников, А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников // Современные тенденции технических наук: материалы Междунар. науч. конф. (г. Уфа, октябрь 2011 г.). – Уфа: Лето, 2011. – С. 8–13.

122. Букалерова, Л. А. Особенности уголовно-правовой охраны информации как предмета хищений / Л. А. Букалерова // Уголовно-правовая политика и проблемы противодействия современной преступности: сборник научных трудов / под ред. д. ю. н., проф. Н. А. Лопашенко. – Саратов: Саратовский Центр по исследованию проблем организованной преступности и коррупции: Сателлит, 2006. – С. 536–545.

123. Букалерова, Л. А. Отсутствие главы в УК «Информационные преступления» – законодательный пробел / Л. А. Букалерова // Пробелы в российском законодательстве. – 2008. – № 1. – С. 256–257.

124. Васенин, В. А. Информационная безопасность и компьютерный терроризм / В. А. Васенин // Научные и методологические проблемы информационной безопасности: сборник статей / под ред. В. П. Шерстюка. – М.: МЦНМО, 2004. – С. 67–83.

125. Вехов, В. Б. Проблемы определения понятия компьютерной информации в свете унификации уголовных законодательств стран СНГ / В. Б. Вехов // Уголовное право. – 2004. – № 4. – С. 15–17.

126. Воробьев, В. В. Вопросы применения состава ст. 274 УК РФ / В. В. Воробьев // Вестник Коми республиканской академии государственной службы и управления. Серия «Государство и право». – 2015. – № 20. – С. 12–18.

127. Герасимова, О. С. Особенности преступлений в сфере компьютерной информации / О. С. Герасимова // Вестник ТГУ. – 2007. – № 12. – С. 327–330.

128. Гончарова, Д. И. Проблематика уголовной ответственности за нарушения правил эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей / Д. И. Гончарова // Международный журнал экспериментального образования. – 2014. – № 6–2. – С. 32–34.

129. Гребеньков, А. А. Общие подходы к определению понятия «компьютерная информация» в уголовно-правовой теории / А. А. Гребеньков // Известия Юго-Западного государственного университета. Серия: История и право. – 2012. – № 1–2. – С. 135–138.

130. Денисов, Н. Л. Концептуальные основы формирования международного стандарта при установлении уголовной ответственности за деяния, связанные с искусственным интеллектом / Н. Л. Денисов // Международное уголовное право и международная юстиция. – 2019. – № 4. – С. 18–20.

131. Денисов, Н. Л. Несоответствие современным реалиям существующей уголовной ответственности за неправомерный доступ к компьютерной информации / Н. Л. Денисов // Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий: сборник материалов межвуз. науч.-практ. конф., 19 апреля 2018 г. – Рязань: Изд-во Рязанского филиала Московского университета МВД России имени В. Я. Кикотя, 2018. – С. 104–107.

132. Денисов, Н. Л., Ромашкина, Н. Ю. Анализ и оптимизация для единообразия правоприменения современного понимания киберпреступления / Н. Л. Денисов, Н. Ю. Ромашкина // Противодействие преступлениям, совершенным с использованием информационно-коммуникационных технологий: сборник материалов межвуз. науч.-практ. конф., 19 апреля 2018 г. – Рязань: Изд-во Рязанского филиала Московского университета МВД России имени В. Я. Кикотя, 2018. – С. 121–126.

133. Денисов, Н. Л., Ромашкина, Н. Ю. Классификация современных киберпреступлений / Н. Л. Денисов, Н. Ю. Ромашкина // Уголовное право и информатизация преступности: проблемы теории, практики и преподавания: сборник статей по материалам Всерос. науч. конф. – М.: Издательский дом «Юриспруденция», 2018. – С. 253–257.

134. Евдокимов, К. Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями / К. Н. Евдокимов // Вестник Казанского юридического института МВД России. – 2016. – № 2. – С. 62–64.

135. Евдокимов, К. Н. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации / К. Н. Евдокимов // Вектор науки ТГУ. Серия: Юридические науки. – 2014. – № 4. – С. 33–36.

136. Ефремова, М. А. Уголовная ответственность за нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений / М. А. Ефремова // Вестник Казанского юридического института МВД России. – 2015. – № 1. – С. 55–58.

137. Ефремова, М. А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ / М. А. Ефремова // Информационное право. – 2015. – № 3. – С. 12–16.

138. Ефремова, М. А. Уголовно-правовая охрана сведении, составляющих коммерческую, банковскую и налоговую тайны / М. А. Ефремова // Вестник Пермского университета. Юридические науки. – 2015. – № 1 (27). – С. 124–132.

139. Ефремова, М. А. Электронный документ как предмет преступления / М. А. Ефремова // Вестник Академии Генеральной прокуратуры Российской Федерации. – 2015. – № 5 (49). – С. 10–15.

140. Ефремова, М. А. Информационная безопасность как объект уголовно-правовой охраны / М. А. Ефремова // Информационное право. – 2014. – № 5. – С. 21–25.

141. Ефремова, М. А. К вопросу об уголовно-правовом обеспечении информационной безопасности / М. А. Ефремова // Вестник Тверского государственного университета. Серия: Право. – 2013. – № 35. – С. 86–91.

142. Ефремова, М. А. Мошенничество с использованием электронной информации / М. А. Ефремова // Информационное право. – 2013. – № 4. – С. 19–21.

143. Ефремова, М. А. Ответственность за неправомерный доступ к компьютерной информации по действующему уголовному законодательству / М. А. Ефремова // Вестник Казанского юридического института МВД России. – 2012. – № 8. – С. 54–56.

144. Журавленко, Н. И. Проблемы борьбы с киберпреступностью и перспективные направления международного сотрудничества в этой

сфере / Н. И. Журавленко, Л. Е. Шведова // Общество и право. – 2015. – № 3. – С. 66–70.

145. Зарубин, С. В. К вопросу об оценке эффективности мероприятий по противодействию информационному терроризму / С. В. Зарубин // Вестник Воронежского института МВД России. – 2008. – № 4. – С. 118–122.

146. Зегжда, П. Д. Современные аспекты обеспечения безопасности информационно-телекоммуникационных систем / П. Д. Зегжда // Проблемы информационной безопасности. Компьютерные системы. – 2002. – № 1. – С. 14–18.

147. Иванов, Н. А. О понятии «цифровые доказательства» и их месте в общей системе доказательств / Н. А. Иванов // Проблемы профилактики и противодействия компьютерным преступлениям: материалы Международной научно-практической конференции (г. Челябинск, 30 мая 2007 г.) и «круглого стола» (г. Челябинск, 18 мая 2007 г.) / отв. ред. А. В. Минбалеев; Челябинский центр по исследованию проблем противодействия организованной преступности и коррупции. – Челябинск, 2008. – С. 96–100.

148. Иванов, С. М. Международно-правовое регулирование борьбы с кибертерроризмом / С. М. Иванов, О. Г. Томило // Право и безопасность. – 2013. – № 3–4. – С. 82–87.

149. Иванченко, Р. Б. Проблемы квалификации мошенничества в сфере компьютерной информации / Р. Б. Иванченко, А. Н. Малышев // Вестник Воронежского института МВД России. – 2014. – № 1. – С. 194–200.

150. Казарин, О. В. Новые разновидности угроз международной информационной безопасности / О. В. Казарин, В. Ю. Скиба, Р. А. Шарыпов // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. – 2016. – № 1. – С. 54–72.

151. Карамнов, А. Ю. Ответственность за создание, использование и распространение вредоносных компьютерных программ по действующему уголовному законодательству / А. Ю. Карамнов // Социально-экономические явления и процессы. – 2012. – № 11. – С. 285–288.

152. Касперский, К. Взлом Пентагона. Как взломать закрытую сеть / К. Касперский // Спецхакер. – 2005. – № 10. – С. 75–76.

153. Качалов, В. В. Международно-правовое регулирование противодействия терроризму / В. В. Качалов // Вестник экономической безопасности. – 2016. – № 1. – С. 89–94.

154. Клименский, М. М. Международно-правовое регулирование противодействия терроризму / М. М. Клименский // Сборники конференций НИЦ Социосфера. – 2014. – № 33. – С. 22–24.

155. Климов, С. М. Методы и интеллектуальные средства предупреждения и обнаружения компьютерных атак на критически важные сегменты информационно-телекоммуникационных систем / С. М. Климов // Известия Таганрогского государственного радиотехнического университета. – 2005. – № 48. – С. 74–82.

156. Ковалев, С. Д. Формирование понятия «специальные технические средства»: исторический, научный и практический аспекты / С. Д. Ковалев, Е. В. Полуянова // Пенитенциарное право: юридическая теория и правоприменительная практика. – 2016. – № 3. – С. 72–76.

157. Ковлагина, Д. А. Информационный терроризм / Д. А. Ковлагина // Вестник Саратовской государственной юридической академии. – 2013. – № 6. – С. 181–184.

158. Козаев, Н. Ш. Несовершенство законодательной техники как негативный фактор развития уголовного законодательства в условиях научно-технического прогресса / Н. Ш. Козаев // Вестник СевКавГТИ. – 2016. – № 1 (24). – С. 82–85.

159. Козаев, Н. Ш. Изменения в уголовной политике в связи с проблемами обеспечения безопасности интернет-пространства / Н. Ш. Козаев // Вестник Санкт-Петербургского университета МВД России. – 2015. – № 1 (65). – С. 48–50.

160. Козаев, Н. Ш. Некоторые вопросы противодействия преступности, использующей достижения научно-технического прогресса / Н. Ш. Козаев // Вестник СевКавГТИ. – 2015. – № 4 (23). – С. 102–104.

161. Козаев, Н. Ш. Уголовная статистика как зеркало общественных отношений, обусловленных научно-техническим прогрессом / Н. Ш. Козаев // Научный вестник Омской академии МВД России. – 2014. – № 4 (25). – С. 3–6.

162. Козаев, Н. Ш. Некоторые проблемы обеспечения информационной безопасности уголовно-правовыми средствами / Н. Ш. Козаев // Вестник СевКавГТИ. – 2014. – № 16. – С. 162–165.

163. Козаев, Н. Ш. Современные информационные технологии как один из факторов развития уголовного права / Н. Ш. Козаев // Вестник Северо-Осетинского государственного университета им. К. Л. Хетагурова. – 2013. – № 3. – С. 87–92.

164. Козаев, Н. Ш. К вопросу о генезисе уголовного права в условиях научно-технического прогресса / Н. Ш. Козаев // Общество и право. – 2012. – № 2 (39). – С. 113–117.

165. Козаев, Н. Ш. Влияние научно-технических достижений на генезис уголовного права / Н. Ш. Козаев // Общество и право. – 2012. – № 5 (42). – С. 127–130.

166. Коломинов, В. В. О способе совершения мошенничества в сфере компьютерной информации / В. В. Коломинов // Человек: преступление и наказание. – 2015. – № 3. – С. 145–149.

167. Коломыченко, М. Киберпреступники сорвали банк / М. Коломыченко // Коммерсантъ. – 2015. – № 213. – С. 1.

168. Конышев, В. Н. Новая военная доктрина Барака Обамы и национальные интересы России / В. Н. Конышев, А. А. Сергунин // Национальные интересы: приоритеты и безопасность. – 2012. – № 14. – С. 2–9.

169. Коржов, В. Электронное правительство против кибертеррористов / В. Коржов // Computerworld Россия. – 2008. – № 4.

170. Котенко, И. В. Таксономии атак на компьютерные системы / И. В. Котенко // Труды СПИИРАН. – 2003. – Т. 2. – № 1. – С. 196–211.

171. Кошечкина, Е. А. К вопросу о противодействии кибертерроризму в Российской Федерации и Республике Узбекистан / Е. А. Кошечкина // The Newman in Foreign Policy. – 2017. – № 39 (83). – С. 40–46.

172. Кошечкина, Е. А. К вопросу о проблемах противодействия кибертерроризму / Е. А. Кошечкина // Омский научный вестник. Серия Общество. История. Современность. – 2017. – № 4. – С. 97–101.

173. Кошечкина, Е. А. К вопросу о проблемах законодательства в сфере кибертерроризма / Е. А. Кошечкина, С. В. Новиков // Омский научный вестник. Серия Общество. История. Современность. – 2017. – № 4. – С. 101–104.

174. Крапивенский, А. С. Информация как товар в XXI веке: анализ угроз безопасности национальным рынкам / А. С. Крапивенский // Информационная безопасность 2010: материалы VII Международной конференции, 15–16 апреля 2010 г. – Кишинев, 2010. – С. 14–17.

175. Кривогин, М. С. Незаконный оборот специальных технических средств: проблемы квалификации преступлений / М. С. Криволгин // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – 2014. – № 2. – С. 110–112.

176. Крутских, А. В. К политико-правовым основаниям глобальной информационной безопасности / А. В. Крутских // Международные процессы. – 2007. – № 13. – С. 28–37.

177. Кузнецов, А. В. Совершенствование правового регулирования уголовной ответственности за отдельные виды мошенничества / А. В. Кузнецов // Научный вестник Омской академии МВД России. – 2014. – № 3. – С. 28–30.

178. Кузнецов, А. П. Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети / А. П. Кузнецов // Правовые вопросы связи. – 2007. – № 2. – С. 25–28.

179. Кузнецова, Н. Ф. Историко-сравнительный анализ уголовно-правовых отраслей науки, законодательства и правоприменения / Н. Ф. Кузнецова // Российский криминологический взгляд. – 2008. – № 1. – С. 124–130.

180. Кургузкина, Е. Б. Место совершения компьютерных преступлений / Е. Б. Кургузкина, Н. Д. Ратникова // Вестник Воронежского института ФСИН России. – 2016. – № 1. – С. 79–87.

181. Кушниренко, С. П. Цифровая информация как самостоятельный объект криминалистического исследования / С. П. Кушниренко // Вестник криминалистики. – М.: Спарк, 2006. – С. 43–47.

182. Лапунин, М. М. Общая характеристика преступлений в сфере компьютерной информации / М. М. Лапунин // Право. Законодательство. Личность. – 2013. – № 1. – С. 36–44.

183. Лахов, В. Г. Содержание понятия «специальные технические средства» в оперативно-розыскной деятельности: научные и нормативные подходы / В. Г. Лахов, С. Д. Ковалев, Е. В. Полуянова // Вестник Международного юридического института. – 2016. – № 1. – С. 32–38.

184. Лопатина, Т. М. Новые виды современной террористической деятельности / Т. М. Лопатина // Современное право. – 2012. – № 4. – С. 122–126.

185. Лопатина, Т. М. Проблемы уголовно-правовой защиты сферы компьютерной информации: современный взгляд на мошенничество / Т. М. Лопатина // Право и безопасность. – 2013. – № 3–4. – С. 89–95.

186. Лопатина, Т. М. Условно-цифровое вымогательство, или кибершантаж / Т. М. Лопатина // Журнал российского права. – 2015. – № 1. – С. 118–126.

187. Лопатина, Т. М. Совершенствование уголовно-правового регулирования использования специальных технических средств, предназначен-

ных для негласного получения информации / Т. М. Лопатина // Российское право: образование, практика, наука. – 2018. – № 4 (106). – С. 75–78.

188. Лопатина, Т. М. Трансформация уголовного права и уголовного процесса в условиях развития цифровых технологий: на примере использования специальных технических средств, предназначенных для негласного получения информации / Т. М. Лопатина // Библиотека криминалиста. Научный журнал. – 2018. – № 3 (38). – С. 64–68.

189. Лопашенко, Н. А. Законодательная реформа мошенничества: вынужденные вопросы и вынужденные ответы / Н. А. Лопашенко // Криминологический журнал Байкальского государственного университета экономики и права. – 2015. – № 3. – С. 504–513.

190. Лопашенко, Н. А. Уголовно-правовая и криминологическая политика государства в области высоких технологий / Н. А. Лопашенко // Сборник научных трудов Международной конференции «Информационные технологии и безопасность». – Киев: Национальная академия наук Украины, 2003. – С. 89–97.

191. Мазуров, В. А. Преступность в сфере высоких технологий: понятие, общая характеристика, тенденции / В. А. Мазуров // Вестник ТГУ. – 2007. – № 1. – С. 151–154.

192. Малюк, А. А. Организационно-методические проблемы обнаружения атак на объекты информационной инфраструктуры кредитно-финансовой сферы / А. А. Малюк // Вопросы кибербезопасности. – 2016. – № 5. – С. 8–14.

193. Маслакова, Е. А. Кибертерроризм как новая форма терроризма / Е. А. Маслакова // Наука и практика. – 2015. – № 2. – С. 79–81.

194. Нагорный, А. А. Содержания понятия компьютерной информации как предмета компьютерных преступлений / А. А. Нагорный // Актуальные проблемы российского права. – 2014. – № 8. – С. 1694–1698.

195. Нечаева, Е. В. Посягательства на цифровую информацию: современное состояние проблемы / Е. В. Нечаева, Э. Ю. Латыпова, Э. М. Гильманов // Человек: преступление и наказание. – 2019. – Т. 27 (1–4), № 1. – С. 80–86.

196. Новиков, В. А. Дискуссионные аспекты определения границ видового объекта преступлений, предусмотренных главой 19 УК РФ / В. А. Новиков // Журнал российского права. – 2016. – № 4. – С. 101–108.

197. Номоконов, В. А. Киберпреступность: прогнозы и проблемы борьбы / В. А. Номоконов, Т. Л. Тропина // Библиотека криминалиста. – 2013. – № 5. – С. 148–160.

198. Олефиренко, С. П. Уголовно-правовое исследование состояния морального вреда в преступлениях, предусмотренных статьями 138, 138.1 Уголовного кодекса Российской Федерации / С. П. Олефиренко // Вестник Челябинского государственного университета. – 2013. – № 5. – С. 90–94.

199. Памазан, С. В. Проблемы современного законодательства в сфере противодействия терроризму / С. В. Памазан // Вестник Владимирского юридического института. – 2006. – № 1. – С. 239–241.

200. Пархомов, В. А. К определению понятия «Информационное преступление» / В. А. Пархомов // Вестник ИГЭА. – 2001. – № 2. – С. 10–14.

201. Пеньков, И. А. Основные направления борьбы с кибертерроризмом / И. А. Пеньков // Мир и Согласие. – 2006. – № 1. – С. 40–44.

202. Петренко, А. А. Киберучения. Методические рекомендации ENISA / А. А. Петренко, С. А. Петренко // Вопросы кибербезопасности. – 2015. – № 3. – С. 2–14.

203. Петроченков, С. Д. Криминологические особенности преступлений в сфере информационно-коммуникационных технологий / С. Д. Петроченков // Вестник Московского университета МВД России. – 2018. – № 6. – С. 155–158.

204. Петроченков, С. Д. Квалификация способов совершения преступления, предусмотренного статьей 183 Уголовного кодекса Российской Федерации / С. Д. Петроченков // Юристъ-Правоведъ. – 2017. – № 1 (80). – С. 59–62.

205. Петроченков, С. Д. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации: законодательный подход и судебная практика / С. Д. Петроченков // Пробелы в российском законодательстве. – 2012. – № 3. – С. 155–157.

206. Петроченков, С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации / С. Д. Петроченков // Вестник Московского университета МВД России. – 2012. – № 6. – С. 72–76.

207. Петроченков, С. Д. К вопросу о предмете преступления, предусмотренного ст. 138.1 Уголовного кодекса Российской Федерации/ С. Д. Петроченков // Труды Академии управления МВД России. – 2016. – № 3 (39). – С. 23–27.

208. Полякова, Т. А. Правовые проблемы установления ответственности за использование информационно-телекоммуникационных систем в террористических и экстремистских целях / Т. А. Полякова, О. В. Тульская // Проблемы правовой информатизации. – 2006. – № 2. – С. 34–36.

209. Пшенко, К. А. Кибертерроризм – угроза международной безопасности / К. А. Пшенко, П. К. Анисимов // Национальная безопасность и стратегическое планирование. – 2015. – № 3. – С. 94–97.

210. Радаев, Н. Н. Рациональная стратегия защиты объекта. Концепция повышения защищенности критически важных объектов от технологического терроризма / Н. Н. Радаев // Безопасность. Достоверность. Информация. – 2007. – № 2. – С. 22–26.

211. Радченко, О. В. Проблемы классификации незаконного оборота специальных технических средств, предназначенных для негласного получения информации / О. В. Радченко, С. В. Габеев // Вестник Восточно-Сибирского института Министерства внутренних дел России. – 2014. – № 3. – С. 26–33.

212. Радько, Н. М. Угрозы непосредственного доступа в операционную среду компьютера / Н. М. Радько, Ю. К. Язов, А. С. Суховеров // Информация и безопасность. – 2007. – № 2. – С. 317–320.

213. Радько, Н. М. Угрозы непосредственного доступа в операционную среду компьютера / Н. М. Радько, Ю. К. Язов, А. С. Суховеров // Информация и безопасность. – 2007. – № 4. – С. 610–611.

214. Решетников, А. Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) / А. Ю. Решетников, Е. А. Русскевич // Законы России: опыт, анализ, практика. – 2018. – № 2. – С. 51–55.

215. Рожков, С. Ю. Кибертерроризм – угроза обществу / С. Ю. Рожков // Материалы XI региональной научно-технической конференции «Вузовская наука – Северо-Кавказскому региону». Том первый: Естественные и точные науки. Технические и прикладные науки. – Ставрополь: СевКавГТУ, 2007. – С. 200–204.

216. Румянцев, К. Е. Защита информации, передаваемой по световодным линиям связи / К. Е. Румянцев, И. Е. Хайров // Информационное противодействие угрозам терроризма. – 2004. – № 2. – С. 27–32.

217. Русскевич, Е. А. Проблемы систематизации современного уголовного законодательства об ответственности за преступления, совершае-

мые с использованием информационно-коммуникационных технологий (ИКТ) / Е. А. Русскевич // Уголовная политика и правоприменительная практика: сб. ст. по мат. VI Международной науч.-практ. конф. – СПб.: Северо-Западный филиал ФГБОУВО «Российский государственный университет правосудия». 2019. – С. 351–358.

218. Рычкалова, Л. А. Биометрические средства идентификации / Л. А. Рычкалова, А. В. Нарижный // Вестник МГОУ. Серия «Юриспруденция». – 2008. – № 3. – С. 38–41.

219. Сабанов, А. Безопасность баз данных / А. Сабанов // Connect!. – 2006. – № 4. – С. 13–14.

220. Савиновский, А. Н. Преступления в сфере компьютерной информации в законодательстве РФ / А. Н. Савиновский // Экономика, социология и право. – 2016. – № 5. – С. 113–116.

221. Савченко, О. А. Совершенствование уголовно-правового законодательства в сфере компьютерной информации на современном этапе развития информационных технологий / О. А. Савченко // Законность и правопорядок в современном обществе. – 2016. – № 29. – С. 156–161.

222. Саломатина, Е. С. Перспективы развития законодательства в сфере борьбы с кибертерроризмом / Е. С. Саломатина // Закон и право. – 2009. – № 1. – С. 47–48.

223. Сальников, А. А. Методологические проблемы противодействия кибертерроризму / А. А. Сальников, В. В. Ященко // Научные и методологические проблемы информационной безопасности: сборник статей / под ред. В. П. Шерстюка. – М.: МЦНМО, 2004. – С. 97–100.

224. Семченков, И. П. Проблемы квалификации заранее обещанных укрывательства и приобретения или сбыта имущества, заведомо добытого преступным путем / И. П. Семченков // Уголовное право. – 2007. – № 3. – С. 56–59.

225. Сердюк, В. А. Некоторые аспекты защиты АСУ ТП / В. А. Сердюк, И. К. Тарви // Information Security / Информационная безопасность. – 2017. – № 6. – С. 12–13.

226. Сивицкая, Н. А. К вопросу об определении понятия «компьютерная информация» / Н. А. Сивицкая // Проблемы правовой информатизации. – 2005. – № 2. – С. 34–36.

227. Сизов, А. В. Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети / А. В. Сизов // Информационное право. – 2007. – № 4. – С. 27–30.

228. Смагин, П. Г. О понятии «компьютерной информации» и особенностях ее использования при расследовании преступлений в ОВД / П. Г. Смагин // Вестник Воронежского института МВД России. – 2008. – № 1. – С. 80–81.

229. Соловьев, В. С. Преступность в социальных сетях Интернета (криминологическое исследование по материалам судебной практики) / В. С. Соловьев // Криминологический журнал Байкальского государственного университета экономики и права. – 2016. – № 1. – С. 60–72.

230. Старичков, М. В. Понятие «компьютерная информация» в российском уголовном праве / М. В. Старичков // Вестник Восточно-Сибирского института МВД России. – 2014. – № 1. – С. 16–20.

231. Степанов-Егиянц, В. Г. Совершение кражи и мошенничества с использованием компьютера или информационно-телекоммуникационных сетей / В. Г. Степанов-Егиянц // Риск: ресурсы, информация, снабжение, конкуренция. – 2012. – № 4. – С. 393–396.

232. Степанов-Егиянц, В. Г. Новая редакция статьи 274 Уголовного кодекса РФ: проблемы и пути решения / В. Г. Степанов-Егиянц // Мониторинг правоприменения. – 2014. – № 2. – С. 18–23.

233. Степанов-Егиянц, В. Г. Безопасное обращение компьютерной информации и проблемы международного правотворчества / В. Г. Степанов-Егиянц // Историческая и социально-образовательная мысль. – 2015. – № 2. – С. 164–170.

234. Сурма, И. В. Цифровая дипломатия в мировой политике / И. В. Сурма// Государственное управление. Электронный вестник. – 2015. – № 49. – С. 220–249.

235. Терещенко, Л. К. Информационная безопасность органов исполнительной власти на современном этапе / Л. К. Терещенко, О. И. Тиунов // Журнал российского права. – 2015. – № 8. – С. 100–109.

236. Титарева, Е. Г. Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий / Е. Г. Титарева // Научный альманах. – 2015. – № 7. – С. 1158–1161.

237. Тропина, Т. Л. Киберпреступность и кибертерроризм: поговорим о понятийном аппарате / Т. Л. Тропина // Сборник научных трудов Международной конференции «Информационные технологии и безопасность». – Киев: Национальная академия наук Украины, 2003. – С. 173–181.

238. Трофимцева, С. Ю. Объект компьютерных преступлений в российском и европейском уголовном праве: сравнительный анализ / С. Ю. Трофимцева, Д. А. Илюшин, А. В. Линьков // Информационное противодействие угрозам терроризма. – 2015. – № 24. – С. 3–11.

239. Трунцевский, Ю. В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов / Ю. В. Трунцевский // Журнал российского права. – 2019. – № 5. – С. 99–106.

240. Тяжлов, И. Хакеры уничтожили сайт «Московского комсомольца» / И. Тяжлов // Коммерсантъ. – 2009. – № 227. – С. 6.

241. Урпин, А. Б. Совершенствование уголовной ответственности за незаконный оборот специальных технических средств, предназначенных для негласного получения информации / А. Б. Урпин // Уголовный закон России: пути развития и проблемы применения: сб. науч. статей / под ред. д-ра юрид. наук, профессора В. И. Тюнина. – СПб.: Изд-во СПбГЭУ, 2013. – С. 253–256.

242. Федулов, В. И. Компьютерный терроризм как инновация современного высокотехнологичного общества / В. И. Федулов // Вестник МГОУ. Серия «Юриспруденция». – 2007. – № 1 (Т. 2). – С. 103–107.

243. Филаненко, А. Ю. Отграничения мошенничества в компьютерной информации от неправомерного доступа / А. Ю. Филаненко // Право и государство: теория и практика. – 2013. – № 1. – С. 59–62.

244. Фролов, Д. Б. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом / Д. Б. Фролов, Е. В. Старостина // Законодательство и экономика. – 2005. – № 5. – С. 62–66.

245. Халиуллин, А. И. Уголовно-правовой аспект неправомерного уничтожения компьютерной информации / А. И. Халиуллин // Вестник Самарской гуманитарной академии. Серия: Право. – 2013. – № 2. – С. 100–105.

246. Харламов, Д. И. Критерии криминализации новых видов мошенничества в УК РФ / Д. И. Харламов // Актуальные вопросы борьбы с преступлениями. – 2016. – № 1. – С. 44–46.

247. Хилюта, В. В. Необходимость установления уголовной ответственности за хищения, совершаемые с использованием компьютерной техники / В. В. Хилюта // Криминологический журнал Байкальского государственного университета экономики и права. – 2012. – № 1. – С. 26–31.

248. Хилюта, В. В. Правовая информатизация и уголовный закон / В. В. Хилюта // Проблемы правовой информатизации. – 2007. – № 1. – С. 74–79.

249. Хисамова, З. И. Уголовная ответственность и искусственный интеллект: теоретические и прикладные аспекты / З. И. Хисамова, И. Р. Бегишев // Всероссийский криминологический журнал. – 2019. – Т. 13, № 4. – С. 564–574.

250. Хисамова, З. И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий / З. И. Хисамова // Общество и право. – 2016. – № 1 (55). – С. 117–120.

251. Хисамова, З. И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий / З. И. Хисамова // Юридический мир. – 2016. – № 2. – С. 58–62.

252. Хисамова, З. И. Неправомерный оборот средств платежей в контексте норм об ответственности за преступления, совершаемые в отношении информационно-коммуникационных технологий / З. И. Хисамова // Общество и право. – 2015. – № 4 (54). – С. 139–144.

253. Хисамова, З. И. Понятие и сущность преступлений, посягающих на информационную безопасность в сфере экономики / З. И. Хисамова // Общество и право. – 2015. – № 1 (51). – С. 157–161.

254. Хисамова, З. И. Способы легализации (отмывания) доходов, полученных преступным путем, с использованием информационно-телекоммуникационных технологий / З. И. Хисамова // Вестник Краснодарского университета МВД России. – 2017. – № 2 (36). – С. 84–87.

255. Хисамова, З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа / З. И. Хисамова // Государство и право. – 2015. – № 3. – С. 127–132.

256. Хисамова, З. И. Уголовно-правовое противодействие новым видам угроз в информационной сфере / З. И. Хисамова // Вестник Краснодарского университета МВД России. – 2015. – № 4 (30). – С. 136–139.

257. Хисамова, З. И. Кардерство в современной России / З. И. Хисамова // Вестник Краснодарского университета МВД России. – 2012. – № 3 (17). – С. 97–100.

258. Хисамова, З. И. Законодательная регламентация уголовной ответственности за преступления, совершаемые в сфере цифровой экономики, в странах Юго-Восточной Азии / З. И. Хисамова // Общественная безопасность, законность и правопорядок в III тысячелетии. – 2018. – № 4–1. – С. 366–370.

259. Хисамова, З. И. Квалификация посягательств, совершенных с использованием электронных средств платежа / З. И. Хисамова // Юридическая наука и правоохранительная практика. – 2015. – № 3 (33). – С. 127–132.

260. Хисамова, З. И. О конструкции норм уголовного законодательства, предусматривающих ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / З. И. Хисамова // Уголовная политика и культура противодействия преступности: материалы Междунар. науч.-практ. конф., 30 сент. 2016 г. – Краснодар: Краснодарский университет МВД России, 2016. – С. 346–350.

261. Хисамова, З. И. Правовое регулирование искусственного интеллекта / З. И. Хисамова, И. Р. Бегишев // Baikal Research Journal. – 2019. – Т. 10, № 2.

262. Черкасов, В. Н. Информационная безопасность. Правовые проблемы и пути их решения / В. Н. Черкасов // Информационная безопасность регионов. – 2007. – № 1. – С. 6–14.

263. Чернядьева, Н. А. О международных подходах правового регулирования борьбы с кибертерроризмом / Н. А. Чернядьева // Информационное право. – 2016. – № 2. – С. 26–29.

264. Чижов, Д. Конец хакерской вольницы / Д. Чижов // Коммерсантъ Деньги. – 2010. – № 40. – С. 38–42.

265. Чупрова, А. Ю. Электронная коммерция как объект уголовно-правовой охраны / А. Ю. Чупрова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2008. – № 1. – С. 98–100.

266. Чупрова, А. Ю. Проблемы использования электронных медицинских карт: уголовно-правовые аспекты / А. Ю. Чупрова // Ученые труды Российской академии адвокатуры и нотариата. – 2014. – № 4. – С. 48–51.

267. Чупрова, А. Ю. Уголовно-правовая оценка мошенничества / А. Ю. Чупрова // Ученые труды Российской академии адвокатуры и нотариата. – 2015. – № 1. – С. 66–70.

268. Чупрова, А. Ю. Проблемы квалификации мошенничества с использованием информационных технологий / А. Ю. Чупрова // Уголовное право. – 2015. – № 5. – С. 131–134.

269. Шерстюк, В. П. Информационная безопасность в системе обеспечения национальной безопасности России, федеральные и региональные аспекты обеспечения информационной безопасности / В. П. Шерстюк // Информационное общество. – 1999. – № 5. – С. 3–5.

270. Шерстюк, В. П. Проблемы противодействия компьютерной преступности и кибертерроризму / В. П. Шерстюк // Материалы четвертой Международной научной конференции по проблемам безопасности и противодействия терроризму. Московский государственный университет им. М. В. Ломоносова. 30–31 октября 2008 г. Том 1: Материалы пленарных заседаний; Материалы первой Всероссийской научно-практической конференции «Формирование устойчивой антитеррористической позиции гражданского общества как основы профилактики терроризма». – М.: МЦНМО, 2009. – С. 43–51.

271. Шеслер, А. В. Мошенничество: проблемы реализации законодательных новелл / А. В. Шеслер // Уголовное право. – 2013. – № 2. – С. 67–71.

272. Шивдяков, Л. А. Особенности критически важных систем и факторы, влияющие на состояние обеспечения безопасности информации в них / Л. А. Шивдяков, В. М. Максимов, Ю. К. Язов // Информация и безопасность. – 2010. – № 2. – С. 243–246.

273. Шутова, А. А. Уголовно-правовая охрана деловой репутации юридических лиц / А. А. Шутова // Вестник Российского университета кооперации. – 2016. – № 3 (25). – С. 140–142.

274. Шутова, А. А. Особенности квалификации незаконного получения сведений, составляющих коммерческую или банковскую тайну / А. А. Шутова // Расследование преступлений: проблемы и пути их решения. – 2016. – № 3 (13). – С. 73–77.

275. Шутова, А. А. Сравнительно-правовой анализ норм об ответственности за информационные преступления по законодательству Республики Казахстан и России / А. А. Шутова // Наука. Мысль. – 2016. – № 9. – С. 142–146.

276. Шутова, А. А. Техника имплементации норм международного права за информационные преступления в законодательство Российской Федерации в контексте интеграции мировых культур / А. А. Шутова // Юридическая техника. –2016. – № 10. – С. 643–647.

277. Шутова, А. А. Информация как конструктивный признак отдельных составов преступлений / А. А. Шутова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2015. – № 2 (30). – С. 201–205.

278. Шутова, А. А. Социальная обусловленность норм об уголовной ответственности за посягательства на экономическую информацию /

А. А. Шутова // Вестник Нижегородской правовой академии. – 2015. – № 4 (4). – С. 73–74.

279. Шутова, А. А. Социальная обусловленность существования норм об уголовной ответственности за посягательства на персональные данные / А. А. Шутова // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2015. – № 4 (32). – С. 332–335.

280. Шутова, А. А. Особенности функциональной роли информации в конструкции отдельных составов преступлений / А. А. Шутова // Материалы XIII Международной научно-практической конференции «Татищевские чтения: актуальные проблемы науки и практики», г. Тольятти, 21–24 апреля 2016 г.: в 5 т. / М-во образования и науки Самарской обл., Мэрия г. о. Тольятти Самарской обл., Univ. degli studi di Brescia (Италия), Волжский ун-т им. В. Н. Татищева. – Тольятти: Волжский ун-т им. В. Н. Татищева, 2016. – 347 с.

281. Шутова, А. А. Распространение сведений как способ совершения информационных преступлений / А. А. Шутова // Материалы Международной научно-практической конференции «Правоохранительная деятельность органов внутренних дел в контексте современных научных исследований», г. Санкт-Петербург, 11 декабря 2015 г. – СПб.: Санкт-Петербургский университет МВД России, 2016. – С. 254–257.

282. Шутова, А. А. Распространение сведений как способ совершения информационных преступлений / А. А. Шутова // Материалы XIV Международной научно-практической конференции «Татищевские чтения: актуальные проблемы науки и практики», г. Тольятти, 20–21 апреля 2017 г.: в 4 т. / М-во образования и науки Самарской обл., Мэрия г. о. Тольятти Самарской обл., Волжский ун-т им. В. Н. Татищева. – Тольятти: Волжский ун-т им. В. Н. Татищева, 2017. – С. 289–292.

283. Щербаков, В. Б. Классификация беспроводных сетей по набору применяемых средств защиты / В. Б. Щербаков // Информация и безопасность. – 2009. – № 1. – С. 125–128.

284. Энгельгардт, А. А. Уголовно-правовая оценка создания, использования и распространения вредоносных компьютерных программ (информации) / А. А. Энгельгардт // Lex Russica. – 2014. – № 11 (т. XCVI). – С. 1316–1325.

Электронные ресурсы

285. DoS-атака // Свободная энциклопедия Википедия. – URL: https://ru.wikipedia.org/wiki/DoS-атака (дата обращения: 23.05.2019).

286. G-DATA // Свободная энциклопедия Википедия. – URL: https://ru.wikipedia.org/wiki/G-DATA (дата обращения: 23.05.2019).

287. Cybercrime Damages $ 6 Trillion By 2021 // Cybersecurity Ventures. – URL: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/ (дата обращения: 23.05.2019).

288. Аналитический отчет «Глобальное исследование утечек конфиденциальной информации в 2018 г.» // Аналитический центр InfoWatch. – URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2018_year.pdf?rel=1 (дата обращения: 23.05.2019).

289. Аналитический отчет «Актуальные киберугрозы. I квартал 2019 года» // Аналитический центр Positive Technologies. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-q1–2019/#id5 (дата обращения: 23.05.2019).

290. Аналитический отчет «Современные угрозы, исходящие от информационных систем» // Аналитический центр InfoWatch. – URL: https://www.infowatch.ru/sites/default/files/docs/pamyatka_sovremenye_ugrozi_IW.pdf (дата обращения: 23.05.2019).

291. Аникеенко, В. Вынесен приговор программисту, пытавшемуся продать секретные сведения // Аналитика по информационной безопасности Anti-Malware.ru. – URL: https://www.anti-malware.ru/news/2015–12–21/2908 (дата обращения: 23.05.2019).

292. Атаманов, Г. А. Методология безопасности / Г. А. Атаманов // Фонд содействия научным исследованиям проблем безопасности «НАУКА-XXI». – URL: http://naukaxxi.ru/materials/302/ (дата обращения: 23.05.2019).

293. Бегишев, И. Р. Безопасность России: вопросы противодействия кибертерроризму / И. Р. Бегишев // Фонд содействия научным исследованиям проблем безопасности «НАУКА-XXI». – URL: http://www.naukaxxi.ru/materials/298 (дата обращения: 23.05.2019).

294. Беспалов, В. Пути совершенствования законодательной системы в борьбе с кибертерроризмом в России и за рубежом // Центр исследования компьютерной преступности. – URL: http://www.crime-research.ru/articles/ceberteror (дата обращения: 23.05.2019).

295. Брандмауэр – это программный и/или аппаратный барьер между двумя сетями, позволяющий устанавливать только авторизованные межсетевые соединения. Брандмауэр защищает соединяемую с Интернетом корпоративную сеть от проникновения извне и исключает возможность доступа к конфиденциальной информации // Словари и энциклопедии на Академике. – URL: http://dic.academic.ru/dic.nsf/fin_enc/20680/Брандмауэр (дата обращения: 23.05.2019).

296. В мире два десятка стран занимаются кибероружием //Портал новостей высоких технологий и науки CyberSecurity.ru. – URL: http://www.cybersecurity.ru/armament/86546.html (дата обращения: 23.05.2019).

297. В Оренбуржье вынесен приговор хакеру // Информационное агентство Regnum. – URL: http://regnum.ru/news/accidents/1257598.html (дата обращения: 23.05.2019).

298. В Пакистане введена смертная казнь за кибертерроризм // Информационный портал по безопасности SecurityLab.ru. – URL: http://www.securitylab.ru/news/362634.php (дата обращения: 23.05.2019).

299. Васильев, В. А. Проблемы развития законодательства в сфере борьбы с киберпреступностью // Центр исследования компьютерной преступности. – URL: http://www.crime-research.ru/ articles/vasil06 (дата обращения: 23.05.2019).

300. Великобритания: данные пациентов продаются на черном рынке // Английская ежедневная газета Daily Mail. – URL: http://www.dailymail.co.uk/news/article-1221186/Private-medical-records-sale-Harley-Street-clinic-patients-files-outsourced-input – end-black-market.html (дата обращения: 23.05.2019).

301. Генпрокуратура: число преступлений в IT-сфере возросло // РосКомСвобода. – URL: https://roskomsvoboda.org/40924 (дата обращения: 23.05.2019).

302. Источник в Минобороны: в Вооруженных силах РФ созданы войска информационных операций // Информационное агентство России ТАСС. – URL: http://tass.ru/politika/1179830 (дата обращения: 23.05.2019).

303. Компьютерные преступления // Словари и энциклопедии на Академике. – URL: http://dic.academic.ru/dic.nsf/ruwiki/977065 (дата обращения: 23.05.2019).

304. Найдена уязвимость в алгоритме, позволяющая прослушивать мобильные телефоны // Информационный портал по безопасности

SecurityLab.ru. – URL: http://www.securitylab.ru/news/389223.php?pagen=2&el_id=389223 (дата обращения: 23.05.2019).

305. Нейтрализация // Словари и энциклопедии на Академике. – URL: http://dic.academic.ru/dic.nsf/bse/166987/Нейтрализация (дата обращения: 23.05.2019).

306. Основные направления научных исследований в области обеспечения информационной безопасности Российской Федерации // Официальный сайт Совета Безопасности Российской Федерации. – URL: http://www.scrf.gov.ru/documents/6/94.html (дата обращения: 23.05.2019).

307. Павлищев, Б. Борьба с кибертерроризмом: у России и США разные подходы // Центр исследования компьютерной преступности. – URL: http://www.crime-research.ru/news/11.03.2009/6436/ (дата обращения: 23.05.2019).

308. Панасенко, А. Мы стоим на пороге кибернетических войн // Информационно-аналитический центр Anti-Malware.ru. – URL: http://www.anti-malware.ru/node/1987 (дата обращения: 23.05.2019).

309. Панасенко, А. В Южной Корее обнаружена самая большая в истории страны утечка личных данных // Аналитика по информационной безопасности Anti-Malware.ru. – URL: https://www.anti-malware.ru/news/2015–12–21/2325 (дата обращения: 23.05.2019).

310. Последние тенденции в использовании научно-технических достижений правонарушителями и компетентными органами, ведущими борьбу с преступностью, в том числе применительно к киберпреступности // Секретариат Организация Объединенных Наций. – URL: http://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_9/V1050384r.pdf (дата обращения: 23.05.2019).

311. Ревич, Ю. Вся правда о кибервойнах // Новая газета. – URL: http://www.novayagazeta.ru/society/41482.html (дата обращения: 23.05.2019).

312. Сегодня кибертерроризм может нанести значительно больший вред, чем обычное взрывное устройство // Официальный сайт ФСБ России. – URL: http://www.fsb.ru/fsb/comment/remark/single.htm! id=10310485@fsb Comment.html (дата обращения: 23.05.2019).

313. Статистика и аналитика // Официальный сайт МВД России. – URL: https://mvd.ru/Deljatelnost/statistics (дата обращения: 23.05.2019).

314. Угланов, Ю. А. Правовые и организационные вопросы борьбы с преступлениями в сфере компьютерной информации в Российской

Федерации // Доклад на VII Международной конференции «Право и Интернет». – URL: http://www.ifap.ru/pi/07 (дата обращения: 23.05.2019).

315. Управление «К» выявило с начала года 7,5 тыс. преступлений в IT-сфере // Центр исследования компьютерной преступности. – URL: http://www.crime-research.ru/news/24.11.2010/7020/ (дата обращения: 23.05.2019).

316. Форум radioscanner.ru. – URL: http://www.radioscanner.ru/forum/topic46225–8.html (дата обращения: 23.05.2019).

317. Хакеры осуществляют 700 тысяч атак в год на государственные интернет-ресурсы // Информационный портал по безопасности SecurityLab.ru. – URL: http://www.securitylab.ru/news/ 297360.php (дата обращения: 23.05.2019).

Книги, монографии, учебники, учебные пособия, словари

318. Батычко, В. Т. Уголовное право. Общая и Особенная части: курс лекций / В. Т. Батычко. – Таганрог: Изд-во ТТИ ЮФУ, 2006. – 668 с.

319. Бикеев, И. И. Материальные объекты повышенной опасности в российском уголовном праве: общие и специальные вопросы / И. И. Бикеев. – Казань: Познание, 2007. – 272 с.

320. Вехов, В. Б. Компьютерные преступления: способы совершения методики расследования / В. Б. Вехов. – М.: Право и закон, 1996. – 182 с.

321. Волеводз, А. Г. Компьютерная информация как объект криминалистического следоведения / А. Г. Волеводз. – М.: Юрлитинформ, 2008. – 401 с.

322. Воройский, Ф. С. Информатика. Энциклопедический словарь-справочник: введение в современные информационные и телекоммуникационные технологии в терминах и фактах / Ф. С. Воройский. – М.: Физматлит, 2006. – 768 с.

323. Гаврилов В. М. Противодействие преступлениям, совершаемым в сфере компьютерной и мобильной коммуникации организованными преступными группами / В. М. Гаврилов. – Саратов: Саратовский Центр по исследованию проблем организованной преступности и коррупции: Сателлит, 2009. – 192 с.

324. Ефремова, М. А. Уголовно-правовая охрана информационной безопасности / М. А. Ефремова. – М.: Юрлитинформ, 2018. – 312 с.

325. Ефремова, М. А. Уголовная ответственность за преступления, совершаемые с использованием информационно-телекоммуникационных технологий / М. А. Ефремова. – М.: Юрлитинформ, 2015. – 200 с.

326. Козаев, Н. Ш. Противодействие злоупотреблениям современными технологиями: международно-правовые и уголовно-правовые аспекты / Н. Ш. Козаев. – М.: Юрлитинформ, 2016. – 192 с.

327. Козаев, Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом / Н. Ш. Козаев. – М.: Юрлитинформ, 2019. – 480 с.

328. Левин, В. И. История информационных технологий. – М.: Бином. Лаборатория Знаний, 2009. – 336 с.

329. Мардер, Н. С. Современные телекоммуникации. – М.: ИРИАС, 2006. – 384 с.

330. Мещеряков, В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. – Воронеж: Изд-во Воронеж. гос. ун-та, 2002. – 408 с.

331. Петроченков, С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации. – М.: ЮНИТИ-ДАНА, 2017. – 135 с.

332. Петроченков, С. Д. Уголовно-правовая защита сведений, составляющих коммерческую, налоговую или банковскую тайну. – М.: ЮНИТИ-ДАНА, 2017. – 81 с.

333. Преступность, уголовная политика, уголовный закон: сб. науч. тр. / под ред. Н. А. Лопашенко; Саратовский Центр по исследованию проблем организованной преступности и коррупции: – Саратов: Изд-во ФГБОУ ВПО «Саратов. гос. юрид. акад.», 2013. – 652 с.

334. Прокис, Дж. Цифровая связь: пер. с англ.; под ред. Д. Д. Кловского / Дж. Прокис. – М.: Радио и связь, 2000. – 800 с.

335. Расследование неправомерного доступа к компьютерной информации / под ред. Н. Г. Шурухнова. – М.: Изд-во «Щит-М», 1999. – 254 с.

336. Русскевич, Е. А. Уголовное право и «цифровая преступность»: проблемы и решения: монография / Е. А. Русскевич. – М.: ИНФРА-М, 2019. – 227 с.

337. Семенов, Г. В. Расследование преступлений в сфере мобильных телекоммуникаций / Г. В. Семенов. – М.: Юрлитинформ, 2006. – 336 с.

338. Скляр, Б. Цифровая связь. Теоретические основы и практическое применение: пер. с англ./ Б. Скляр. –2-е изд., испр. – М.: Издательский дом «Вильямс», 2003. – 1104 с.

339. Скляров, Д. В. Искусство защиты и взлома информации. – СПб.: БХВ-Петербург, 2004. – 288 с.

340. Хисамова, З. И. Уголовная ответственность за преступления, совершаемые в финансовой сфере с использованием информационно-телекоммуникационных технологий / З. И. Хисамова. – М.: Юрлитинформ, 2017. – 160 с.

341. Хисамова, З. И. Международный опыт уголовно-правового противодействия преступлениям в сфере цифровой экономики / З. И. Хисамова. – Краснодар: Изд-во Краснодар. ун-та МВД России, 2018. – 119 с.

342. Шутова, А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности / А. А. Шутова. – М.: Юрлитинформ, 2019. – 192 с.

343. Ярочкин, В. И. Информационная безопасность: учебник для вузов. – М.: Летописец, 2000. – 398 с.

Диссертации и авторефераты диссертаций

344. Айсанов, Р. М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: автореф. дис. … канд. юрид. наук: 12.00.08 / Айсанов Руслан Мухамедович. – М., 2006. – 31 с.

345. Бегишев, И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: автореф. дис. … канд. юрид. наук: 12.00.08 / Бегишев Ильдар Рустамович. – Казань, 2017. – 31 с.

346. Бегишев, И. Р. Понятие и виды преступлений в сфере обращения цифровой информации: дис. … канд. юрид. наук: 12.00.08 / Бегишев Ильдар Рустамович. – Казань, 2017. – 204 с.

347. Букалерова, Л. А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: автореф. дис. … д-ра юрид. наук: 12.00.08 / Букалерова Людмила Александровна. – М., 2007. – 66 с.

348. Бытко, С. Ю. Некоторые проблемы уголовной ответственности за преступления, совершенные с использованием компьютерных тех-

нологий: дис. … канд. юрид. наук: 12.00.08 / Бытко Сергей Юрьевич. – Саратов, 2002. – 204 с.

349. Геллер, А. В. Уголовно-правовые и криминологические аспекты обеспечения защиты электронной информации и Интернета: автореф. дис. … канд. юрид. наук: 12.00.08 / Геллер Артем Владимирович. – М., 2006. – 24 с.

350. Григорьев, О. В. Роль и уголовно-процессуальное значение компьютерной информации на досудебных стадиях уголовного судопроизводства: автореф. дис. … канд. юрид. наук: 12.00.09 / Григорьев Олег Геннадьевич. – Омск, 2007. – 24 с.

351. Добровольский, Д. В. Актуальные проблемы борьбы с компьютерной преступностью: автореф. дис. … канд. юрид. наук: 12.00.08 / Добровольский Дмитрий Владимирович. – М., 2005. – 24 с.

352. Ефремова, М. А. Уголовно-правовая охрана информационной безопасности: дис. … д-ра юрид. наук: 12.00.08 / Ефремова Марина Александровна. – М., 2017. – 427 с.

353. Ефремова, М. А. Уголовно-правовая охрана информационной безопасности: автореф. дис. … д-ра юрид. наук: 12.00.08 / Ефремова Марина Александровна. – М., 2017. – 59 с.

354. Зигура, Н. А. Компьютерная информация как вид доказательств в уголовном процессе России: автореф. дис. … канд. юрид. наук: 12.00.09 / Зигура Надежда Анатольевна. – Челябинск, 2010. – 21 с.

355. Зинина, У. В. Преступления в сфере компьютерной информации в российском и зарубежном праве: автореф. дис. … канд. юрид. наук: 12.00.08 / Зинина Ульяна Викторовна. – М., 2007. – 34 с.

356. Зубова, М. А. Компьютерная информация как объект уголовно-правовой охраны: автореф. дис. … канд. юрид. наук: 12.00.08 / Зубова Марина Александровна. – Казань, 2008. – 28 с.

357. Кабанова, А. Ж. Преступления в сфере компьютерной информации (уголовно правовые и криминологические аспекты): автореф. дис. … канд. юрид. наук: 12.00.08 / Кабанова Анна Жунусовна. – Ростов н/Д, 2004. – 24 с.

358. Карпов, В. С. Уголовная ответственность за преступления в сфере компьютерной информации: автореф. дис. … канд. юрид. наук: 12.00.08 / Карпов Виктор Сергеевич. – Красноярск, 2002. – 27 с.

359. Козаев, Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом: автореф. дис. … д-ра юрид. наук: 12.00.08 / Козаев Нодар Шотаевич. – Краснодар, 2016. – 62 с.

360. Козаев, Н. Ш. Современные проблемы уголовного права, обусловленные научно-техническим прогрессом: дис. … д-ра юрид. наук: 12.00.08 / Козаев Нодар Шотаевич. – Краснодар, 2016. – 630 с.

361. Крапивина, О. Н. Приобретение или сбыт имущества, заведомо добытого преступным путем: сравнительно-правовое, уголовно-правовое, уголовно-политическое и криминологическое исследование: автореф. дис. … канд. юрид. наук: 12.00.08 / Крапивина Ольга Николаевна. – М., 2008. – 30 с.

362. Красненкова, Е. В. Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами: автореф. дис. … канд. юрид. наук: 12.00.08 / Красненкова Елена Валерьевна. – М., 2006. – 29 с.

363. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере: автореф. дис. … д-ра юрид. наук: 12.00.14 / Куняев Николай Николаевич. – М., 2010. – 55 с.

364. Лопатина, Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дис. … д-ра юрид. наук: 12.00.08 / Лопатина Татьяна Михайловна. – М., 2006. – 418 с.

365. Лопатина, Т. М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: автореф. дис. … д-ра юрид. наук: 12.00.08 / Лопатина Татьяна Михайловна. – М., 2006. – 60 с.

366. Маляров, А. И. Уголовно-правовые и криминологические аспекты международного сотрудничества в сфере защиты электронно-цифровой информации: автореф. дис. … канд. юрид. наук: 12.00.08 / Маляров Андрей Иванович. – Краснодар, 2008. – 26 с.

367. Медведев, С. С. Мошенничество в сфере высоких технологий: автореф. дис. … канд. юрид. наук: 12.00.08 / Медведев Сергей Сергеевич. – Краснодар, 2008. – 21 с.

368. Мнацаканян, А. В. Информационная безопасность Российской Федерации: уголовно-правовые аспекты: дис. … канд. юрид. наук: 12.00.08 / Мнацаканян Аревик Васильевна. – М., 2015. – 216 с.

369. Петроченков, С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации: автореф. дис. … канд. юрид. наук: 12.00.08 / Петроченков Сергей Дмитриевич. – М., 2013. – 20 с.

370. Петроченков, С. Д. Уголовная ответственность за незаконный оборот специальных технических средств, предназначенных для негласного

получения информации: дис. … канд. юрид. наук: 12.00.08 / Петроченков Сергей Дмитриевич. – М., 2013. – 174 с.

371. Степанов-Егиянц, В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): дис. … д-ра юрид. наук: 12.00.08 / Степанов-Егиянц Владимир Георгиевич. – М., 2016. – 389 с.

372. Тропина, Т. Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: автореф. дис. … канд. юрид. наук: 12.00.08 / Тропина Татьяна Львовна. – Владивосток, 2005. – 28 с.

373. Хисамова, З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: автореф. дис. … канд. юрид. наук: 12.00.08 / Хисамова Зарина Илдузовна. – Краснодар, 2016. – 32 с.

374. Хисамова, З. И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий: дис. … канд. юрид. наук: 12.00.08 / Хисамова Зарина Илдузовна. – Краснодар, 2016. – 222 с.

375. Шутова, А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты: автореф. дис. … канд. юрид. наук: 12.00.08 / Шутова Альбина Александровна. – Н. Новгород, 2017. – 22 с.

376. Шутова, А. А. Уголовно-правовое противодействие информационным преступлениям в сфере экономической деятельности: теоретический и прикладной аспекты: дис. … канд. юрид. наук: 12.00.08 / Шутова Альбина Александровна. – Н. Новгород, 2017. – 264 с.

377. Чупрова, А. Ю. Уголовно-правовые механизмы регулирования отношений в сфере электронной коммерции: дис. … д-ра юрид. наук: 12.00.08 / Чупрова Антонина Юрьевна. – М., 2015. – 607 с.

378. Шагинян, Г. А. Антитеррористическая информационная политика Российского государства: автореф. дис. … канд. полит. наук: 23.00.02 / Шагинян Гаянэ Артуровна. – Краснодар, 2006. – 24 с.

379. Щепетильников, В. Н. Уголовно-правовая охрана электронной информации: автореф. дис. … канд. юрид. наук: 12.00.08 / Щепетильников Виктор Николаевич. – Елец, 2006. – 24 с.

380. Юрченко, И. А. Информация конфиденциального характера как предмет уголовно-правовой охраны: автореф. дис. … канд. юрид. наук: 12.00.08 / Юрченко Ирина Александровна. – М., 2000. – 24 с.

381. Яшков, С. А. Информация как объект преступления: автореф. дис. … канд. юрид. наук: 12.00.08 / Яшков Сергей Александрович. – Екатеринбург, 2005. – 26 с.

Материалы судебной практики

382. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации): Постановление Пленума Верховного Суда Российской Федерации № 46 от 25 декабря 2018 г. // Российская газета. – 2019. – № 1.

383. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда Российской Федерации № 48 от 30 ноября 2017 г. // Российская газета. – 2017. – № 280.

384. По делу о проверке конституционности части третьей статьи 138 Уголовного кодекса Российской Федерации в связи с жалобами граждан С. В. Капорина, И. В. Коршуна и других: Постановление Конституционного Суда Российской Федерации № 3-П от 31 марта 2011 г. // Собрание законодательства Российской Федерации. – 2011. – № 15. – Ст. 2191.

385. Приговор Андроповского районного суда Ставропольского края от 31 октября 2014 г. по уголовному делу № 1–97/2014. – URL: https://rospravosudie.com/court-andropovskij-rajonnyj-sud-stavropolskij-kraj-s/act-461098820/ (дата обращения: 23.05.2019).

386. Приговор Октябрьского районного суда г. Тамбова от 9 июля 2010 г. по уголовному делу № 1–331/2010. – URL: http://sud23.tmb. sudrf.ru/modules.php?name=information&id=1242 (дата обращения: 23.05.2019).

387. Приговор Октябрьского районного суда г. Кирова от 13 июля 2016 г. по уголовному делу № 1–298/2016. – URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-532913468/ (дата обращения: 23.05.2019).

388. Приговор Трусовского районного суда г. Астрахани от 25 марта 2010 г. – URL: http://trusovsky.ast.sudrf.ru/modules.php?id=356&name=docum_sud (дата обращения: 23.05.2019).

389. Приговор Надымского городского суда Ямало-Ненецкого автономного округа от 18 августа 2010 г. по уголовному делу № 1–248/2010. – URL: https://rospravosudie.com/court-nadymskij-gorodskoj-sud-yamalo-neneckij-avtonomnyj-okrug-s/act-104979780 (дата обращения: 23.05.2019).

390. Приговор Вяземского городского суда Смоленской области от 24 декабря 2010 г. по уголовному делу № 1–258/2010. – URL: https://rospravosudie.com/court-vyazemskij-rajonnyj-sud-smolenskaya-oblast-s/act-100135204 (дата обращения: 23.05.2019).

391. Приговор Промышленного районного суда г. Оренбурга от 21 февраля 2011 г. по уголовному делу № 1–55/2011. – URL: https://rospravosudie.com/court-promyshlennyj-rajonnyj-sud-g-orenburga-oren-burgskaya-oblast-s/act-100557127 (дата обращения: 23.05.2019).

392. Приговор Чкаловского районного суда г. Екатеринбурга от 13 октября 2011 г. по уголовному делу № 1–749/2011. – URL: https://rospravosudie.com/court-chkalovskij-rajonnyj-sud-g-ekaterinburga-sverd-lovskaya-oblast-s/act-103444196 (дата обращения: 23.05.2019).

393. Приговор Чистопольского городского суда Республики Татарстан от 4 мая 2012 г. по уголовному делу № 1–80/12. – URL: https://rospravosudie.com/court-chistopolskij-gorodskoj-sud-respublika-tatarstan-s/act-104673919/ (дата обращения: 23.05.2019).

394. Приговор Белебеевского городского суда Республики Башкортостан от 20 июня 2012 г. по уголовному делу № 1–111/2012. – URL: https://rospravosudie.com/court-belebeevskij-gorodskoj-sud-respublika-bashkor-tostan-s/act-106616429 (дата обращения: 23.05.2019).

395. Приговор Октябрьского районного суда г. Кирова от 29 июня 2012 г. по уголовному делу № 1–139/2012. – URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-105417412 (дата обращения: 23.05.2019).

396. Приговор Авиастроительного районного суда г. Казани Республики Татарстан от 17 апреля 2012 г. по уголовному делу № 90/12. – URL: https://rospravosudie.com/court-aviastroitelnyj-rajonnyj-sud-g-kazani-respublika-tatarstan-s/act-105043335/ (дата обращения: 23.05.2019).

397. Приговор Кировского районного суда г. Томска от 18 января 2013 г. по уголовному делу № 1–41/2013. – URL: https://rospravosudie.com/court-kirovskij-rajonnyj-sud-g-tomska-tomskaya-oblast-s/act-107259596 (дата обращения: 23.05.2019).

398. Приговор мирового судьи судебного участка № 45 Егорьевского судебного района Московской области Евменьева В. А. от 13 февраля 2013 г. по уголовному делу № 1–12/2013. – URL: https://rospravosudie.com/court-sudebnyj-uchastok-45-mirovogo-sudi-egorevskogo-sudebnogo-rajona-moskovskoj-oblasti-s/act-209063908 (дата обращения: 23.05.2019).

399. Приговор мирового судьи судебного участка № 213 Раменского судебного района Московской области Гаврилова Ж. А. от 2 февраля 2014 г. по уголовному делу № 1–20/2014. – URL: https://rospravosudie.com/court-sudebnyj-uchastok-213-mirovogo-sudi-ramenskogo-sudebnogo-rajona-moskovskoj-oblasti-s/act-214545153 (дата обращения: 23.05.2019).

400. Приговор мирового судьи судебного участка № 2 г. Костромы Суслова Е. А. от 16 мая 2014 г. по уголовному делу № 1–11/2014. – URL: https://rospravosudie.com/court-sudebnyj-uchastok-mirovogo-sudi-2-po-g-kostrome-s/act-215471248 (дата обращения: 23.05.2019).

401. Приговор Ленинского районного суда г. Махачкала от 7 сентября 2015 г. по уголовному делу № 1–357/2015. – URL: https://rospravosudie.com/court-leninskij-rajonnyj-sud-g-maxachkaly-respublika-dagestan-s/act-496771870 (дата обращения: 23.05.2019).

402. Приговор Советского районного суда г. Орска, Оренбургской области от 15 сентября 2015 г. по уголовному делу № 1–303/2015. – URL: https://rospravosudie.com/court-sovetskij-rajonnyj-sud-g-orska-orenburgskaya-oblast-s/act-498742768 (дата обращения: 23.05.2019).

403. Приговор Промышленного районного суда г. Самары от 22 апреля 2016 г. по уголовному делу № 1–219/2016. – URL: https://rospravosudie.com/court-promyshlennyj-rajonnyj-sud-g-samary-samarskaya-oblast-s/act-524031536 (дата обращения: 23.05.2019).

404. Приговор Центрального районного суда г. Оренбурга от 28 июня 2016 г. по уголовному делу № 1–246/2016. – URL: https://rospravosudie.com/court-centralnyj-rajonnyj-sud-g-orenburga-orenburgskaya-oblast-s/act-532247401 (дата обращения: 23.05.2019).

405. Приговор Ленинского районного суда г. Кирова от 9 июня 2010 г. по уголовному делу № 1–395/2010. – URL: https://rospra-vosudie.com/court-leninskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-100771110 (дата обращения: 23.05.2019).

406. Приговор Якутского городского суда Республики Саха (Якутия) от 8 ноября 2010 г. по уголовному делу № 1–1639/2010. – URL:

https://rospravo–sudie.com/court-yakutskij-gorodskoj-sud-respublika-saxa-yakuti-ya-s/act-100271062 (дата обращения: 23.05.2019).

407. Приговор Набережночелнинского городского суда Республики Татарстан от 13 октября 2010 г. по уголовному делу № 1–1487/10. – URL: https://rospravosudie.com/court-naberezhnochelninskij-gorodskoj-sud-respublika-tatarstan-s/act-106458840/ (дата обращения: 23.05.2019).

408. Приговор Завьяловского районного суда Удмуртской Республики от 29 июня 2011 г. по уголовному делу № 1–131/2011. – URL: https://rospravosudie.com/court-zavyalovskij-rajonnyj-sud-udmurtskaya-respub-lika-s/act-101685242 (дата обращения: 23.05.2019).

409. Приговор Первомайского районного суда г. Ижевска от 29 июня 2011 г. по уголовному делу № 1–187/2011. – URL: https://rospravo-sudie.com/court-pervomajskij-rajonnyj-sud-g-izhevska-udmurtskaya-respublika-s/act-103503226 (дата обращения: 23.05.2019).

410. Приговор Комсомольского районного суда г. Тольятти Самарской области от 27 апреля 2012 г. по уголовному делу № 1–227/2012. – URL: https://rospravosudie.com/court-komsomolskij-rajonnyj-sud-g-tolyatti-samarskaya-oblast-s/act-104750802 (дата обращения: 23.05.2019).

411. Приговор Орджоникидзевского районного суда г. Екатеринбурга от 23 июля 2012 г. по уголовному делу № 1–429/2012. – URL: https://rospravosudie.com/court-ordzhonikidzevskij-rajonnyj-sud-g-ekaterinburga-sverdlovskaya-oblast-s/act-106337351 (дата обращения: 23.05.2019).

412. Приговор Оренбургского районного суда Оренбургской области от 24 апреля 2013 г. по уголовному делу № 1–160/2013. – URL: https://rospravosudie.com/court-orenburgskij-rajonnyj-sud-orenburgskaya-oblast-s/act-428466358 (дата обращения: 23.05.2019).

413. Приговор Советского районного суда г. Томска от 21 мая 2013 г. по уголовному делу № 1–174/2013. – URL: https://rospravosudie.com/court-sovetskij-rajonnyj-sud-g-tomska-tomskaya-oblast-s/act-107327401 (дата обращения: 23.05.2019).

414. Приговор Энгельсского районного суда Саратовской области от 19 декабря 2014 г. по уголовному делу № 1–767/2014. – URL: https://rospravosudie.com/court-engelsskij-rajonnyj-sud-saratovskaya-oblast-s/act-527260013 (дата обращения: 23.05.2019).

415. Приговор Кировского районного суда г. Самары от 25 ноября 2014 г. по уголовному делу № 1–726/2014. – URL: https://rospravosudie.com/

court-kirovskij-rajonnyj-sud-g-samary-samarskaya-oblast-s/act-464360418 (дата обращения: 23.05.2019).

416. Приговор Северского городского суда Томской области от 6 апреля 2015 г. по уголовному делу № 1–117/2015. – URL: https://rospravosudie.com/court-severskij-gorodskoj-sud-tomskaya-oblast-s/act-488174757 (дата обращения: 23.05.2019).

417. Приговор Первомайского районного суда г. Ижевска от 17 июня 2015 г. по уголовному делу № 1–290/2015. – URL: https://rospravosudie.com/court-pervomajskij-rajonnyj-sud-g-izhevska-udmurtskaya-respublika-s/act-495329927 (дата обращения: 23.05.2019).

418. Приговор Минусинского городского суда Красноярского края от 7 апреля 2016 г. по уголовному делу № 1–26/2016. – URL: https://rospravosudie.com/court-minusinskij-gorodskoj-sud-krasnoyarskij-kraj-s/act-529759028 (дата обращения: 23.05.2019).

419. Приговор Октябрьского районного суда г. Кирова от 13 июля 2016 г. по уголовному делу № 1–298/2016. – URL: https://rospravosudie.com/court-oktyabrskij-rajonnyj-sud-g-kirova-kirovskaya-oblast-s/act-532913468 (дата обращения: 23.05.2019).

420. Приговор Кировского районного суда г. Саратова от 22 июня 2012 г. по уголовному делу № 1–168/2011. – URL: https://rospravosudie.com/court-kirovskij-rajonnyj-sud-g-saratova-saratovskaya-oblast-s/act-100230383 (дата обращения: 23.05.2019).

421. Приговор Чкаловского районного суда г. Екатеринбурга Свердловской области от 22 июня 2012 г. по уголовному делу № 1–395/2012. – URL: https://rospravosudie.com/court-chkalovskij-rajonnyj-sud-g-ekaterinburga-sverdlovskaya-oblast-s/act-107020393 (дата обращения: 23.05.2019).

422. Приговор Нерюнгринского городского суда Республики Саха (Якутия) от 30 мая 2012 г. по уголовному делу № 1–198/2012. – URL: https://rospravosudie.com/court-neryungrinskij-gorodskoj-sud-respublika-saxa-yakutiya-s/act-105926175 (дата обращения: 23.05.2019).

ПРИЛОЖЕНИЯ

Приложение № 1

АНКЕТА ЭКСПЕРНОГО ОПРОСА

Уважаемые коллеги! Целью исследования является выработка научно и практически обоснованных предложений и рекомендаций по совершенствованию российского уголовного законодательства, предусматривающего ответственность за преступления в сфере обращения цифровой информации, а также обеспечение единообразия правопонимания и правоприменения в данной сфере.

Нас интересует ваше мнение. Пожалуйста, прочитайте внимательно вопросы и отметьте подходящий ответ любым знаком.

Спасибо за участие в нашем исследовании!

Вопрос № 1. Является ли термин «цифровая информация» более широким по содержанию, чем термин «компьютерная информация», а термин «информационно-телекоммуникационные устройства, их системы и сети» более широким по содержанию, чем термин «машинный носитель, электронно-вычислительная машина (ЭВМ), системы ЭВМ и их сеть»?

Ответы:

Да

Нет

Затрудняюсь ответить

Вопрос № 2. Считаете ли вы, что под преступлением в сфере обращения цифровой информации необходимо понимать предусмотренное уголовным законом виновное совершенное общественно опасное деяние, направленное на нарушение конфиденциальности, целостности, достоверности и доступности охраняемой законом цифровой информации?

Ответы:

Да

Нет

Затрудняюсь ответить

Вопрос № 3. Целесообразно ли установление уголовной ответственности за незаконные приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем?

Ответы:

Да

Нет

Затрудняюсь ответить

Вопрос № 4. Следует ли принять Федеральный закон «О специальных технических средствах», обеспечивающий системное государственное регулирование правоотношений, возникающих при обороте специальных технических средств, предназначенных для нарушения систем защиты цифровой информации и негласного получения цифровой информации?

Ответы:

Да, необходимо

Нет необходимости

Затрудняюсь ответить

Вопрос № 5. Следует ли установить повышенную уголовную ответственность за преступления в сфере компьютерной информации, сопряженные посягательства на информационно-телекоммуникационные устройства, системы и сети критически важных и потенциально опасных объектов (аэропортов, вокзалов, ядерных и химических станций, энергетических и транспортных предприятий, информационных систем органов государственной власти)?

Ответы:

Да, необходимо

Нет необходимости

Затрудняюсь ответить

Вопрос № 6. Следует ли установить повышенную уголовную ответственность за преступления в сфере компьютерной информации, повлекшие по неосторожности причинение тяжкого вреда здоровью, смерть человека, смерть двух и более лиц, крупный ущерб либо иные тяжкие последствия?

Ответы:

Да, необходимо

Нет необходимости

Затрудняюсь ответить

Вопрос № 7. Согласны ли вы с предложением об установлении повышенной уголовной ответственности за применение технических средств, используемых для негласного получения информации, при нарушении

неприкосновенности частной жизни (ст. 137 УК РФ), воспрепятствовании осуществлению избирательных прав или работе избирательной комиссии (ст. 141 УК РФ), незаконном получении и разглашении сведений, составляющих коммерческую, налоговую и банковскую тайну (ст. 183 УК РФ)?

Ответы:

Да

Нет

Затрудняюсь ответить

Вопрос № 8. Целесообразно ли установление уголовной ответственности за незаконные изготовление, сбыт или приобретение специальных технических средств, предназначенных для нарушения систем защиты цифровой информации (парольные взломщики, обходчики и блокировщики межсетевых экранов и антивирусов, клавиатурные шпионы, взломщики систем криптозащиты и т.д.)?

Ответы:

Да, необходимо

Нет необходимости

Затрудняюсь ответить

Вопрос № 9. Следует ли установить уголовную ответственность за незаконный перехват цифровой информации?

Ответы:

Да

Нет

Затрудняюсь ответить

Вопрос № 10. Считаете ли вы целесообразным с позиции совершенствования системы обеспечения информационной безопасности объединение подразделений различных специальных служб России (МВД, ФСБ, ФСО, МО, СВР и др.) в единую структуру, например в Федеральную службу информационной безопасности Российской Федерации?

Ответы:

Да

Нет

Затрудняюсь ответить

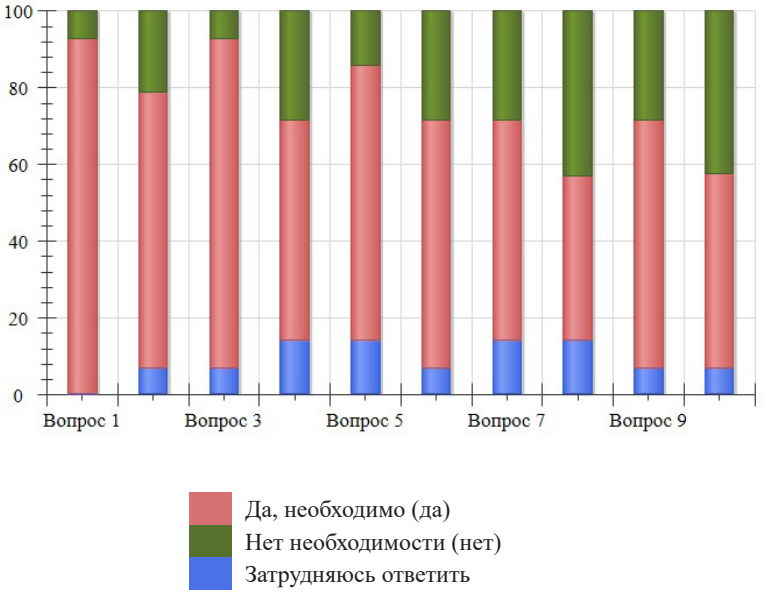
Приложение № 2

Таблица результатов эксперного опроса

Вопросы исследования	Да, необходимо (да) (%)	Нет необходимости (нет) (%)	Затрудняюсь ответить (%)
Вопрос № 1	92,86	7,14	0
Вопрос № 2	71,43	21,43	7,14
Вопрос № 3	85,71	7,14	7,15
Вопрос № 4	57,14	28,57	14,29
Вопрос № 5	71,43	14,29	14,28
Вопрос № 6	64,29	28,57	7,14
Вопрос № 7	57,14	28,57	14,29
Вопрос № 8	42,86	42,86	14,28
Вопрос № 9	64,29	28,57	7,14
Вопрос № 10	50	42,86	7,14

Приложение № 3

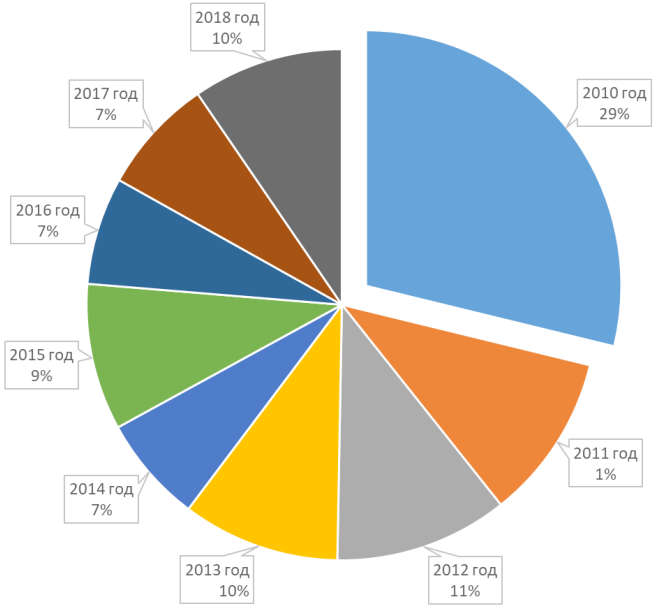
Диаграмма результатов эксперного опроса



Приложение № 4

Сведения о зарегистрированных в Российской Федерации преступлениях в сфере компьютерной информации

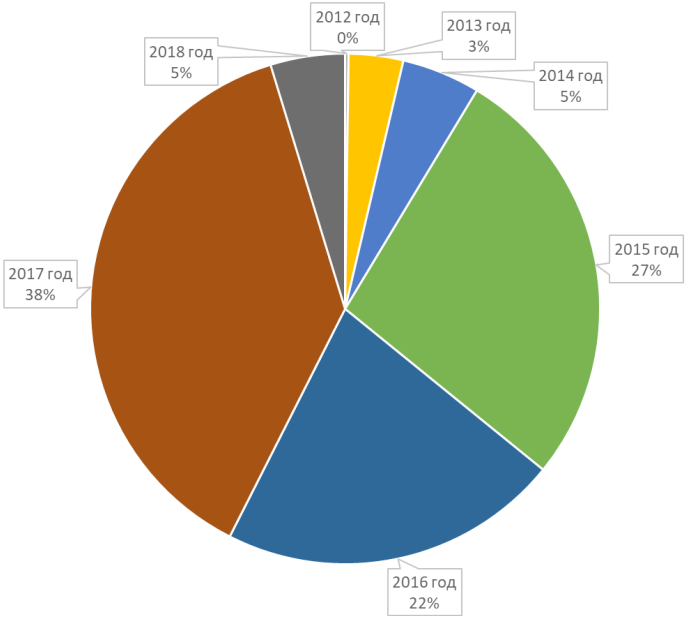
	Годы								
	2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Количество зарегистрированных преступлений	7 398	2 698	2 820	2 563	1 739	2 382	1 748	1 883	2 454



Приложение № 5

Сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 159.6 УК РФ

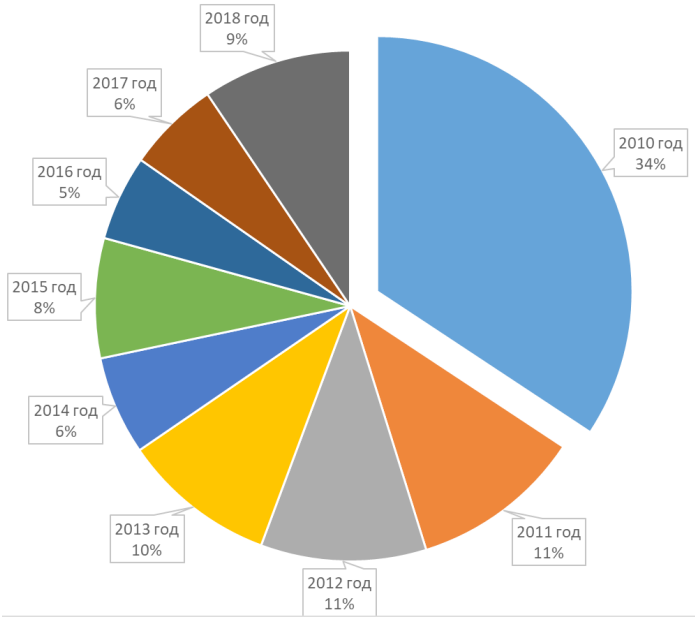
	Годы						
	2012	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Количество зарегистрированных преступлений	43	693	995	5 443	4 329	7 564	946



Приложение № 6

Сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 272 УК РФ

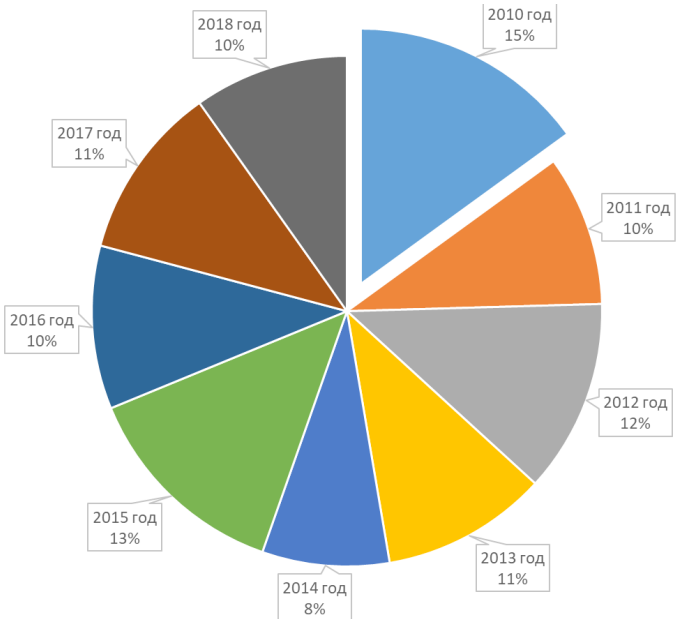
	Годы								
	2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Количество зарегистрированных преступлений	6 309	2 005	1 930	1 799	1 151	1 396	994	1 079	1 737



Приложение № 7

Сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 273 УК РФ

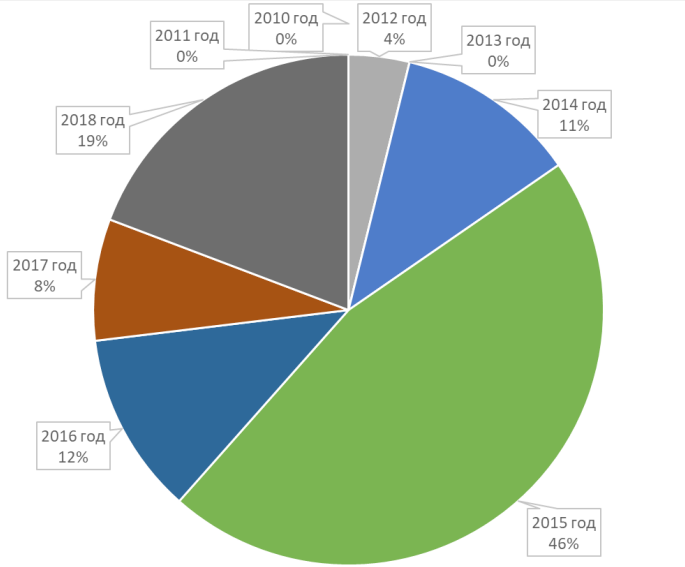
	Годы								
	2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Количество зарегистрированных преступлений	1 089	693	889	764	585	974	751	802	406



Приложение № 8

Сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 274 УК РФ

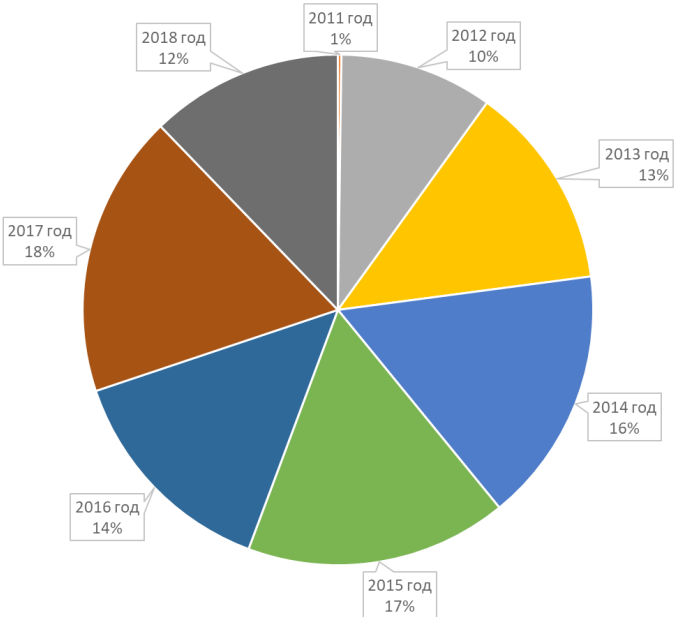
	Годы								
	2010	**2011**	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Количество зарегистрированных преступлений	0	0	1	0	3	12	3	2	5



Приложение № 9

Сведения о зарегистрированных в Российской Федерации преступлениях, предусмотренных ст. 138.1 УК РФ

	Годы							
	2011	**2012**	**2013**	**2014**	**2015**	**2016**	**2017**	**2018**
Количество зарегистрированных преступлений	5	220	294	367	376	321	406	277



Научное издание

Серия «Цифровая безопасность»

БЕГИШЕВ Ильдар Рустамович

БИКЕЕВ Игорь Измаилович

ПРЕСТУПЛЕНИЯ В СФЕРЕ ОБРАЩЕНИЯ ЦИФРОВОЙ ИНФОРМАЦИИ

Главный редактор Г. Я. Дарчинова
Редакторы: Л. Ш. Андурская, Г. А. Тарасова
Технический редактор О. А. Аймурзаева
Дизайнер обложки А. А. Бондаренко

ISBN 978-5-8399-0726-3

Подписано в печать 20.12.2019. Формат 60x84 1/16
Гарнитура Times NR, 11. Усл. печ. л. 17,44. Уч.-изд. л. 13,42
Тираж 1000 экз. Заказ № 155

Издательство Казанского инновационного университета им. В. Г. Тимирясова
420111, г. Казань, ул. Московская, 42. Тел. (843) 231-92-90. E-mail: zaharova@ieml.ru

Отпечатано с готового оригинал-макета в типографии ООО «ТЦО «Таглимат»
420108, г. Казань, ул. Зайцева, 17.