ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОСТОЧНО-СИБИРСКИЙ ИНСТИТУТ МИНИСТЕРСТВА
ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

Родивилин Иван Петрович

УГОЛОВНО-ПРАВОВОЕ И КРИМИНОЛОГИЧЕСКОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ОБРАЩЕНИЯ ОХРАНЯЕМОЙ ЗАКОНОМ ИНФОРМАЦИИ

Специальность 12.00.08 – Уголовное право и криминология;
уголовно-исполнительное право

Диссертация
на соискание ученой степени кандидата юридических наук

Научный руководитель:
доктор юридических наук,
профессор
Репецкая Анна Леонидовна

Иркутск – 2021

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. Массовая цифровизация всех сфер общественной жизни в Российской Федерации в последние десятилетия имеет серьезные негативные последствия в виде появления совершенно нового вида преступности, посягающего на охраняемую законом информацию. Данная проблема не имеет в настоящее время адекватного решения, так как не исследована в полной мере и становится все более острой для современного общества. Актуальность исследования противодействия преступлениям, совершенным в сфере обращения охраняемой законом информации, обусловлена, с одной стороны, ценностью нарушаемого объекта, с другой – сложностью его защиты, связанной с толкованием оценочных признаков при квалификации этих преступлений.

В действующем Уголовном кодексе Российской Федерации установлена уголовная ответственность за совершение преступлений в сфере обращения охраняемой законом информации, однако нет единого толкования понятий, четкой структуры указанных преступлений; существует противоречие в диспозициях уголовно-правовых норм, их регламентирующих. В существующей уголовно-правовой доктрине нет четкого понимания компьютерной информации как предмета преступного посягательства, не решена проблема толкования понятий: «компьютерная информация», «электронная информация», «цифровая информация», «охраняемая законом информация», и их соотношения. Также остаются нерешенными проблемы, возникающие при квалификации преступлений в указанной сфере, связанные с определением места совершения преступления, предметом преступления, оценкой наступивших последствий и т.д.

В новой Доктрине информационной безопасности Российской Федерации, утвержденной Указом Президента РФ, четко указано, что обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при

использовании информационных технологий, является национальным интересом Российской Федерации в информационной сфере[1].

За последние несколько лет преступность, посягающая на информацию, охраняемую законом, изменилась и проникла в различные сферы общественной жизни, о чем свидетельствует увеличение регистрации таких преступлений, как нарушение неприкосновенности частной жизни, нарушение тайны переписки и телефонных переговоров. На десятикратный рост количества регистрируемых «информационных» преступлений за прошедшие 6 лет обратил внимание Президент Российской Федерации, выступая на расширенном заседании коллегии МВД России по итогам работы за 2020 год[2].

В связи с небольшим периодом, в течение которого наблюдаются значительные количественные и качественные изменения характеристики названных преступлений, криминологические исследования их специфики немногочисленны, а вследствие нечеткого определения понятийного аппарата «информационных» преступлений их результаты являются несопоставимыми.

Таким образом, и в современной уголовно-правовой доктрине, и в криминологии отсутствует единый подход к пониманию и изучению рассматриваемой проблемы. Вышеизложенные обстоятельства, как представляется, свидетельствуют об актуальности настоящего исследования и необходимости проведения юридического анализа для разработки уголовно-правового и криминологического противодействия преступлениям в сфере обращения охраняемой законом информации.

Степень научной разработанности темы исследования. За последние 20 лет проблема противодействия преступлениям в сфере обращения охраняемой законом информации рассматривалась в теоретических и практических аспектах, изучалась многими учеными-правоведами.

---

[1] Доктрина информационной безопасности Российской Федерации: утв. Указом Президента РФ от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50, ст. 7074.

[2] Заседание коллегии МВД России // kremlin.ru. URL: http://kremlin.ru/events/president/news/62860.

Большой вклад в исследование различных аспектов противодействия преступлениям в сфере компьютерной информации был сделан такими отечественными учеными, как: Ю.М. Батурин, В.М. Быков, В.Б. Вехов, А.Г. Волеводз, М.С. Гаджиев, О.А. Герасимова, А.Ю. Головин, В.А. Голубев, М.Ю. Дворецкий, Д.В. Добровольский, Р.И. Дремлюга, К.Н. Евдокимов, У.В. Зинина, Д.Н. Карпова, Н.Н. Ковалева, Д.А. Овсюков, А.Л. Осипенко, В.Г. Степанов-Егиянц, А.В. Суслопаров, С.И. Ушаков, А.И. Халлиулин, И.Г. Чекунов, В.В. Челноков, В.Н. Черкасов, П.А. Чирков, С.С. Шахрай, А.Н. Яковлев и др.

Вопросы уголовно-правовой охраны частной жизни исследовались в диссертациях Н.Г. Беляевой, И.П. Галыгиной, В.П. Жеребкина, Б.Н. Кадникова, Е.Е. Калашниковой, В.Н. Клочкова, О.А. Мотина, Г.Б. Романовского, А.М. Ульянченко, И.А. Шевченко и др.

В юридической литературе общие проблемы защиты информации анализировались в работах С.А. Гончарова, Р.Б. Иванченко, Ю.В. Дубровского, В.Н. Лопатина, Н.А. Лопашенко, С.В. Максимова, В.Н. Протасова, А.А. Фатьянова, С.Л. Цаластиной и др.

Проблемы, возникающие в связи с совершением преступлений в сфере обращения электронной и цифровой информации, рассматривались в работах С.И. Гутника, И.Р. Бегишева, Р.Р. Гайфутдинова, М.А. Ефремовой, М.А. Хурум, В.Н. Щепетильникова и др.

Кроме того, уголовно-правовые аспекты преступлений в сфере компьютерной информации отражены в работах Ю.В. Добрынина, В.Г. Жиделева, М.А. Зубовой, В.С. Карпова, В.В. Крылова, Т.М. Лопатиной, Е.А. Лысак, М.М. Малыковцева, Е.А. Маслаковой, В.А. Мещерякова, В.А. Номоконова, А.Б. Попова, М.А. Простосердова, И.А. Сало, О.М. Сафонова, С.П. Спириной, М.В. Старичкова, Т.Л. Тропиной.

Необходимо отметить тот факт, что, несмотря на высокий научно-теоретический и практический уровень исследований указанных авторов,

развитие рассматриваемых отношений идет очень быстрыми темпами. В этой связи возникает ряд проблем уголовно-правового и криминологического содержания, которые остаются нерешенными, что, в свою очередь, негативно сказывается на правоприменительной практике. Таким образом, возникает объективная потребность в проведении комплексного и всестороннего исследования преступлений в сфере обращения охраняемой законом информации в целях разработки уголовно-правовых и криминологических мер, направленных на противодействие указанным преступлениям.

Цель диссертационного исследования состоит в выявлении проблем квалификации, а также особенностей криминологической характеристики преступлений, совершаемых в сфере обращения охраняемой законом информации, позволяющих совершенствовать исследуемые нормы уголовного законодательства и предложить иные меры противодействия преступлениям в сфере обращения охраняемой законом информации.

Для достижения указанных целей поставлены и решены следующие **задачи**:

– обосновать применение термина «охраняемая законом информация ограниченного доступа», раскрыть ее понятие, определить виды и предложить их классификацию; кроме того, сформулировать определение понятия «преступление в сфере обращения охраняемой законом информации»;

– осуществить уголовно-правовой анализ составов преступлений, предусматривающих ответственность за преступления в сфере обращения охраняемой законом информации по российскому законодательству;

– исследовать состояние, структуру и динамику совершения преступлений в сфере обращения охраняемой законом информации;

– дать криминологическую характеристику личности преступника и факторов, детерминирующих совершение преступлений в сфере обращения охраняемой законом информации;

– разработать и обосновать конкретные предложения и рекомендации по совершенствованию уголовного законодательства и иных нормативно-правовых

актов, связанных с совершением преступлений в сфере обращения охраняемой законом информации;

– предложить комплекс мер предупреждения преступлений в сфере обращения охраняемой законом информации.

Научная новизна исследования заключается в том, что в нем выявлены проблемы противодействия преступлениям в сфере обращения охраняемой законом информации в современный период и предложены пути их преодоления. Полученные результаты исследования позволили обосновать целый ряд предложений, связанных с совершенствованием как действующего уголовного законодательства, так и практики его применения (введено понятие «пользовательская информация», разработаны дефиниции «охраняемая законом информация», «неправомерный доступ к охраняемой законом информации» и др.). В рамках настоящего исследования были определены основные особенности преступлений в сфере обращения охраняемой законом информации, предложена типология личности преступника. На основе последней предложена система критериев классификации лиц, совершающих деяния рассматриваемого вида. В научный оборот впервые введено понятие преступлений в сфере оборота охраняемой законом информации, обосновано применение указанного понятия в Уголовном кодексе Российской Федерации и науке криминологии. Выявлено значение различных факторов, влияющих на совершение преступлений в сфере оборота охраняемой законом информации в современной России, отражены изменения в способах совершения таких преступлений за последние годы.

Теоретическая значимость результатов диссертационного исследования состоит в том, что в нем развивается уголовно-правовая доктрина преступлений, совершенных в сфере обращения охраняемой законом информации, и сформулированы выводы, которые могут быть использованы в дальнейших исследованиях указанного объекта.

Практическая значимость исследования заключается в том, что его результаты, разработанные теоретические положения, выводы и рекомендации

могут быть использованы в процессе совершенствования соответствующих норм уголовного законодательства Российской Федерации, в правоприменительной деятельности, а также при осуществлении предупреждения преступлений, совершенных в сфере обращения охраняемой законом информации. Кроме того, представленные результаты могут использоваться в учебном процессе при преподавании как основных курсов по уголовному праву и криминологии, так и специальных курсов по квалификации указанных преступлений и их предупреждению.

Методологическую основу диссертационного исследования составляет диалектический метод познания, позволяющий объективно и всесторонне рассмотреть проблемы юридической оценки преступлений, совершаемых в сфере обращения охраняемой законом информации. Кроме того, в исследовании использованы: метод системного анализа, сравнительно-правовой, исторический, формально-логический, логико-юридический и др.

Методику исследования составили статистический метод, ряд социологических методов, в частности, метод экспертных оценок, а также опрос респондентов в виде анкетирования и формализованного интервью, метод изучения документов. Кроме того, применялся метод включенного наблюдения в период работы соискателя в должности старшего оперуполномоченного отдела «К» (по борьбе с преступлениями в сфере информационных технологий) БСТМ ГУ МВД России по Иркутской области.

Основные положения, выносимые на защиту:

1. Под преступлением в сфере обращения охраняемой законом информации предлагается понимать виновно совершенное общественно опасное деяние, посягающее на общественные отношения, возникающие по поводу охраны информации ограниченного доступа. Признаками такой информации является то, что ее владелец предпринял действия по защите данной информации; и она подпадает под сведения ограниченного доступа, режим оборота которых регулируется Конституцией РФ или федеральными законами.

Понятие «охраняемая законом информация», за нарушение оборота которой предусмотрена уголовная ответственность, является родовым по отношению к таким ее разновидностям, как «аналоговая информация», «цифровая информация», «компьютерная информация», «электронная информация» и другие виды информации. Синонимия понятий, определяющих разновидности охраняемой законом информации, ведет к неоправданному сужению признаков объективной стороны преступления, предусмотренного ст. 272 УК РФ. Они отражают только специфическую форму охраняемой законом информации, устройство, на котором она хранится, или способ ее обработки. Учитывая, что информация ограниченного доступа в любом ее виде должна охраняться законом, нет необходимости выделения из нее отдельных категорий в виде компьютерной, электронной или цифровой информации.

2. Предметом преступления в сфере обращения охраняемой законом информации следует признавать любую информацию, которая охраняется законом. Благодаря этому будет достигаться унификация и единообразие терминов и определений на законодательном уровне. Охраняемая законом информация ограниченного доступа как предмет преступного посягательства – это сведения, защищенные владельцем информации от неправомерного доступа, на которые распространяется режим ограниченного доступа, установленный Конституцией РФ и Федеральными законами.

Под неправомерным доступом к охраняемой законом информации предлагается понимать возможность воздействия на информацию лицом, не имеющим легального права на ознакомление с ней, либо имеющим такое право, но использующим его в нарушение правил доступа к информации в личных интересах или из корыстной заинтересованности. Поскольку общественная опасность неправомерного доступа к пользовательской информации близка по своей сути к неправомерному доступу к персональным данным, предлагается признавать пользовательскую информацию предметом уголовно-правовой охраны и соответственно регламентировать указанное положение в ФЗ «О персональных

данных». Под пользовательской информацией следует понимать совокупность информации, собираемой о пользователях в сети Интернет. К такой информации могут относиться: маршруты передвижений; биометрические данные; покупки; видеозаписи камер наблюдений; сведения об интересах и предпочтениях пользователей (фотографии, имена, даты рождения, адрес проживания, номера телефонов, интересы, поисковые запросы).

Преступления в сфере обращения охраняемой законом информации, предусмотренные УК РФ, можно классифицировать следующим образом: 1) преступления, направленные на получение неправомерного доступа к охраняемой законом информации (статьи 272, 273, 274, 274.1 УК РФ); 2) квалифицированные составы преступлений в сфере обращения охраняемой законом информации (статьи 137, 138, 155, 183, 275, 276, 283, 283.1, 310, 311, 320 УК РФ); 3) преступления против собственности, которые направлены на получение доступа к охраняемой законом информации и с ее помощью хищения денежных средств (статьи 158, 159, 159.3, 159.6 УК РФ); 4) иные преступления, предусмотренные Особенной частью УК РФ, где информация может выступать предметом преступного посягательства или способом совершения преступлений.

3. Динамика состояния исследуемых преступлений имеет крайне неблагоприятный характер, так как их абсолютное количество за исследуемый период увеличилось в 40 раз. В общей структуре зарегистрированных преступлений их удельный вес составляет – 25 %, больше половины (58,8%) совершается с использованием сети «Интернет». Такой рост произошел за счет увеличения числа хищений денежных средств, совершенных с использованием информационно-телекоммуникационных технологий. Именно эти преступления доминируют в структуре, их удельный вес составляет 80,4%. Среди других исследуемых преступлений отмечен значительный рост нарушений неприкосновенности частной жизни (ст. 137 УК РФ) и нарушений тайны переписки, телефонных переговоров и иных сообщений (ст. 138 УК РФ), абсолютные показатели которых увеличились в 3 раза.

В структуре исследуемых преступлений, изученных по способу их совершения, доминировало использование вредоносных компьютерных программ для мобильных телефонов (55 % исследованных случаев); каждым десятым было: использование вредоносных компьютерных программ для неправомерного доступа к компьютерной технике (11 %); неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам (11 %); кардинг[1] (10 %); скимминг[2] (9 %); наименее распространенным способом совершения была ddos-атака[3] – 4 % случаев.

4. Исследование личности преступника, совершающего преступления в сфере обращения охраняемой законом информации, позволило выявить следующие типичные черты большинства из них. Это лица мужского пола (99 %), среди которых преобладают молодые люди в возрасте от 19 до 24 лет (56,1%); 64,7% имеют высшее или среднее образование. По роду занятий каждый пятый из них – это учащийся или студент, 9,4% – программисты; у более чем половины лиц, совершивших исследуемые преступления, работа (обучение) так или иначе были связаны с компьютерными технологиями (54,2 %). Кроме того, достаточные познания в области информационных технологий имели 82,1% осужденных. Большинство преступников проживало в крупных городах, как правило, центрах регионов Российской Федерации (73,1%). Многие из них (87 %) знали об ответственности за совершение указанных преступлений, однако частная превенция здесь не сработала.

Полагаем, что к лицам, совершающим преступления в сфере обращения охраняемой законом информации, применим термин «информационные воры», поскольку их целью является похищение информации. Информационные воры являются частью отдельной категории преступников, которых принято называть

---

[1] Похищение реквизитов, идентифицирующих пользователей в сети Интернет как владельцев банковских кредитных карт, с их возможным последующим использованием для совершения незаконных финансовых операций (покупка товаров либо отмывание денег)

[2] Похищение реквизитов платежной карты с помощью устройства, которое прикрепляется к банкомату и считывает информацию с банковской карты.

[3] Создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён.

киберпреступниками. На основе проведенного криминологического исследования предложена следующая классификация «информационных воров»: 1) лица, использующие вредоносные компьютерные программы для мобильных телефонов; 2) лица, использующие вредоносные компьютерные программы для неправомерного доступа к компьютерам, ноутбукам и т.д.; 3) осуществляющие неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам; 4) совершающие хищение «цифровой личности»; 5) кардеры; 6) лица, совершающие хищение денежных средств, используя «Скиммер»; 7) лица, осуществляющие Ddos-атаки.

5. Выявлены группы факторов, детерминирующих преступность в сфере оборота охраняемой законом информации. Основными группами детерминант являются: факторы правового характера (отсутствие механизма регулирования сети Интернет; отсутствие единого понятийного аппарата при определении преступлений, совершенных в сфере обращения охраняемой законом информации, отсутствие уголовной ответственности за ограничение доступа к охраняемой законом информации); технические факторы (рост числа устройств, подключенных к сети Интернет, увеличение объемов информации, недостаточность защиты самих технических устройств; анонимность пользователей сети Интернет); организационные факторы (неконтролируемый доступ сотрудников к внутренней сети организации; низкий профессионализм или отсутствие служб информационной безопасности; недостаточное финансирование мероприятий по защите информации; низкий уровень специальной подготовки должностных лиц правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере обращения охраняемой законом информации); социально-экономические факторы (возможность получения сверхприбыли при минимальных затратах и минимальном риске при совершении преступлений в сфере оборота охраняемой законом информации; усиление цифрового неравенства); виктимологические факторы (небрежность в работе пользователей информации, их неосмотрительное поведение, выражающееся в

установлении простых паролей для защиты информации и нарушении сроков их использования, либо отсутствие средств защиты информации, а также знаний по защите информации). Выявленные в ходе диссертационного исследования факторы позволили разработать меры специально-криминологического противодействия.

6. Для предупреждения указанных преступлений наиболее действенными представляются меры специально-криминологического предупреждения, которые можно разделить на следующие группы:

– правовые меры (предложение о включении в УК РФ понятия неправомерного доступа к охраняемой законом информации, а также понятия общественно опасных последствий в виде блокирования, модификации, копирования и ограничения доступа к охраняемой законом информации);

– технические (реализация комплекса мер по борьбе с анонимностью пользователей в сети Интернет; введение информационных систем, обрабатывающих большие объемы данных; создание информационной базы данных о вредоносных компьютерных программах; использование операторами связи интернет-протокола Ipv6 по предоставлению телекоммуникационных услуг на территории Российской Федерации с полным отказом от технологии NAT);

– организационные (налаживание должного государственного регулирования за пунктами коллективного доступа в сеть Интернет; включение в реестр запрещённых сайтов специфических интернет-ресурсов, на которых происходит обмен информацией о способах совершения преступлений в сфере обращения охраняемой законом информации; подготовка компетентных сотрудников правоохранительных органов с достаточным уровнем знаний в сфере информационных технологий);

– социально-экономические (отслеживание денежных потоков в сети Интернет (в том числе взаимодействие с интернет-биржами по обмену криптовалют на другие средства платежа); борьба с цифровым неравенством);

– виктимологические (информирование граждан о необходимости и способах соблюдения информационной безопасности, через популярные интернет-ресурсы, телевидение; повышение технического уровня пользователей сети Интернет).

Степень достоверности исследования. Эмпирическую базу исследования составили:

– статистические данные о зарегистрированных преступлениях в сфере компьютерной информации за период с 2010 по 2020 гг.;

– результаты изучения материалов 411 уголовных дел о преступлениях, совершенных в сфере обращения охраняемой законом информации, рассмотренных судами 73 субъектов Российской Федерации в 2006-2020 годах;

– результаты изучения 220 материалов доследственных проверок преступлений в сфере обращения охраняемой законом информации в Иркутской области, Республике Бурятия, Калининградской области, Забайкальском и Хабаровском краях, Челябинской области;

– результаты анкетирования 102 сотрудников подразделений по борьбе с преступлениями в сфере информационных технологий (Управление «К» БСТМ МВД России и их территориальные подразделения) из 40 субъектов Российской Федерации, следователей органов внутренних дел и следственного комитета из 10 субъектов Российской Федерации, деятельность которых связана с расследованием преступлений в сфере электронной информации;

– результаты анкетирования 250 студентов вузов г. Иркутска юридического профиля и обучающихся по направлениям информационной безопасности;

– результаты других исследований в области информационной безопасности.

Апробация результатов исследования. Основные теоретические положения и выводы диссертационного исследования отражены автором в 22 научных публикациях (общим объемом 7,8 п.л.), из которых 6 публикаций в

ведущих рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Минобрнауки России для опубликования основных научных результатов диссертационных исследований.

Результаты исследования и отдельные положения диссертации апробировались автором на 6 международных, всероссийских научных и научно-практических конференциях и круглых столах: «Правозащитная деятельность органов государственной власти: проблемы и перспективы» (Иркутск, 2012); «Уголовная политика и проблемы правоприменения» (Санкт-Петербург, 2013); «Криминалистические чтения на Байкале – 2015» (Иркутск, 2015); IV Всероссийская научно-практическая конференция «Проблемы современного российского законодательства» (Иркутск, 2015); «Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования» (Иркутск, 2017), «Современность в творчестве начинающего исследователя» (Иркутск, 2021), «Деятельность правоохранительных органов в современных условиях» (Иркутск, 2021).

Структура диссертации определена с учетом целей и задач исследования. Диссертационное исследование выполнено в объеме, соответствующем требованиям ВАК при Минобрнауки России. Диссертация состоит из введения, четырех глав, объединяющих девять параграфов, заключения, списка использованных источников и приложений.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИЗУЧЕНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ОХРАНЯЕМОЙ ЗАКОНОМ ИНФОРМАЦИИ

§ 1. Понятие охраняемой законом информации

Со времен первобытного общества до современной цивилизации человечество нуждается в необходимом и важном ресурсе – информации. Известно, что произошедшая в конце 20 века массовая информатизация общества, превратила информацию в повседневную среду для общения между людьми, получения знаний. Важно отметить, что, не обладая достаточным объемом информационных ресурсов, трудно занимать достойное место в современном обществе. Вместе с тем, информация становится товаром, который возможно купить, продать, обменять, похитить и т.д.

Процесс оборота информации в Российской Федерации регулируется Федеральным законом Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[1] (далее – ФЗ № 149-ФЗ), в котором закрепляются основные понятия: информация, электронный документ и др. Вместе с тем, отсутствие четкого понятийного аппарата, имеющего отношение к охраняемой законом информации и совершение в отношении нее преступлений, дает возможность манипулировать понятиями, вводить в заблуждение следствие и суд, тем самым уходить от уголовной ответственности.

Законодатели называют информацию и компьютерной, и цифровой, и электронной, и электронно-цифровой, как пример, отражение в федеральных законах понятия электронно-цифровой подписи или электронный документ.

---

[1] Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защиты информации»: в ред. Федерального закона от 3 апреля 2020 г. № 105-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3448.

Отсутствие систематизации норм, регулирующих совокупность охраняемой законом информации, путаница в определениях, попытка отображения информации через устройство, в котором она находится, отрицательно сказываются на процессе применения уголовно-правовых норм в сфере обращения охраняемой законом информации.

В ст. 2 ФЗ № 149-ФЗ закреплено понятие информации – это сведения (сообщения, данные) независимо от формы их представления, а в примечании 1 к ст. 272 УК РФ дается понятие именно компьютерной информации – сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Слово компьютер упоминается еще в 1897 году в Оксфордском словаре английского языка[1]. Российское законодательство не содержит легальной дефиниции данного понятия. Подобного рода пробел усложняет толкование и использование правоприменителем понятия «компьютерная информация». Термин «компьютерная информация» в современном научном словоупотреблении весьма многозначен и уже не относится к одному понятию компьютер, а распространяется на многие другие современные электронные устройства. Стоит обратить внимание на то, что компьютерная информация может находиться не только в компьютере, но и в периферийных устройствах (принтеры, сканеры и т.д.), телефонных аппаратах, планшетах, а также в киберпространстве (на сервере хостинг-провайдера[2] или социальной сети[3]).

Как показывает изучение доследственных материалов, по которым вынесены постановления об отказе в возбуждении уголовного дела – большая их часть основывается на том обстоятельстве, что компьютерная информация, которая стала предметом преступного посягательства, не признается таковой.

---

[1] Оксфордский словарь английского языка (Oxford English Dictionary) // oed.com. URL: http://www.oed.com/view/Entry/37975.

[2] Хостинг-провайдер – это организация, предоставляющая дисковое пространство и мощности сервера для размещения сайта в сети Интернет.

[3] Социальная сеть – онлайн-платформа, которая используется для общения, знакомств, создания социальных отношений между людьми, которые имеют схожие интересы или офлайн-связи, а также для развлечения (музыка, фильмы) и работы.

Например, если был осуществлен неправомерный доступ к информации, расположенной в учетной записи социальной сети или к электронному почтовому ящику, то эта информация не признается компьютерной. В этом случае выносится постановление об отказе в возбуждении уголовного дела.

Ряд ученых[1] подвергают определение компьютерной информации данное в Уголовном кодексе Российской Федерации критике, обосновывая это тем, что для передачи электронной информации могут быть использованы не только электрические сигналы, но и световые сигналы или электромагнитное излучение, имея ввиду оптоволоконный кабель[2], с помощью которого возможна передача данных. Для уяснения смысла, вкладываемого в понятие «компьютерная информация», необходимо вернутся к формулировке, закрепленной в УК РФ, где законодатель указал, что форма передачи информации не имеет значения. Другими словами, компьютерная информация может передаваться любым способом, в том числе и по оптоволоконному кабелю. Ключевой аспект, по мнению автора, заключается в том, чтобы переданная информация могла быть обработана и преобразована средствами электронной техники, а способ ее доставки от пункта А в пункт Б не влияет на ее свойства.

Однако, у определения «компьютерная информация», данного в Уголовном Кодексе Российской Федерации есть другие недостатки, подробно описанные в работах российских ученых.[3] Исправить рассматриваемые ими неточности можно,

---

[1] См. *Богданова Т.Н.* К вопросу об определении понятия «Преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. 2012. № 37 (291). С. 64; *Жиделев В.Г.* Некоторые аспекты квалификации преступлений в сфере компьютерной информации в российском и зарубежном законодательстве // Человек: преступление и наказание. 2012. № 2. С. 24; Качество уголовного закона: проблемы Особенной части: монография / отв. ред. А. И. Рарог. М.: Проспект, 2017. С. 295.

[2] Оптическое волокно – нить из оптически прозрачного материала (стекло, пластик), используемая для переноса света внутри себя посредством полного внутреннего отражения.

[3] *Бегишев И.Р.* Понятие и виды преступлений в сфере обращения цифровой информации: дис. ... канд. юрид. наук. М., 2017; *Чупрова А.Ю.* Проблемы квалификации мошенничества с использованием информационных технологий // Уголовное право. 2015. № 5. С. 132; *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.

если заменить указанную дефиницию на «цифровую информацию», изучение которой наблюдается в последние годы в работах некоторых ученных[1].

Например, Н.А. Иванов под цифровой информацией понимает любую информацию в виде дискретных сигналов любой физической природы, зафиксированную на машинных носителях, в том числе на носителях, доступ к которым осуществляется с использованием информационно-телекоммуникационных сетей (включая сеть Интернет)[2]. Бегишев И.Р. указывает на то, что понятие «цифровая информация» прочно вошло в нашу повседневную жизнь (цифровое фото, цифровое видео, цифровая связь и д.р.) и предлагает заменить в примечании к ст. 272 УК РФ компьютерную информацию на цифровую.

Ряд авторов в своих работах указывают на то обстоятельство, что с технической точки зрения, в информационных системах и устройствах, в том числе и беспроводных, обращается не компьютерная, а электронная информация[3].

Ученые-процессуалисты уже давно используют термин «электронная информация», к примеру, в качестве доказательств по уголовным делам[4]. Анализ имеющихся научных публикаций, а также материалов следственной и судебной

---

[1] *Бегишев И.Р.* Указ. соч. С. 9-40; Рудых А.А. Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юрид. наук. Ростов-на-Дону, 2020. С. 15.

[2] *Щепетильников В.Н.* Уголовно-правовая охрана электронной информации: автореф. дис. … канд. юрид. наук. Елец, 2006. С. 7; *Ефремова М.А.* Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук. М., 2017. С. 55-56; *Титарева Е.Г.* Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий // Научный альманах. 2015. № 7. С. 1160.

[3] *Иванов Н.А.* Цифровая информация в уголовном процессе // Библиотека криминалиста. 2013. №5 (10). С. 100.

[4] *Александров А.С., Кувычков С.И.* О надежности электронных доказательств в уголовном процессе // Библиотека криминалиста. 2013. № 5(10). С. 76; *Белкин А.Р.* Теория доказывания в уголовном судопроизводстве. М., 2005. С. 56; *Вехов В.Б.* Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. 2013. № 10. С. 22; *Иванов Н.А.* Криминалистические классификации цифровой информации // Вестник Омской юридической академии. 2013. № 1(20). С. 81; *Осипенко А.Л.* Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. 2009. № 4 (35). С. 31; *Полевой Н.С.* Криминалистическая кибернетика. М., 1982. С. 61; *Ткачев А.В.* Использование электронных (компьютерных) документов в качестве документов-доказательств и письменных доказательств в процессуальных отношениях // Библиотека криминалиста. 2013. № 5 (10). С. 128.

практики свидетельствует о том, что электронные доказательства (электронная информация) стали все чаще использоваться по уголовным делам.

А.В. Суслопаров понимает под электронной информацией сведения, не имеющие физических характеристик, хранящиеся на материальном носителе и передающиеся посредством сигналов в форме определённого кода[1]. Как уже было рассмотрено выше информация обладает физическими характеристиками, поэтому не согласимся с этим определением.

Также существует подход по определению компьютерной информации через способ обработки указанной информации, где предметом преступных посягательств против информации предлагается признавать компьютерную информация, вредоносную компьютерную программу или иную компьютерную информацию подобного рода, средства хранения, обработки или передачи компьютерной информации, информационные-телекоммуникационные сети, оконечное оборудование, объекты критической информационной инфраструктуры Российской Федерации, информационные системы, автоматизированные системы управления, сети электросвязи[2].

Вклад вышеперечисленных ученых в разработку понятийного аппарата несомненно велик, однако, по нашему мнению, значимых отличий между компьютерной информации от электронной, цифровой, или электронно-цифровой, нет. Происходит перифраза понятия, попытка дать определение и определить свойства информации через ее носитель или способ обработки и воспроизводства, при этом не обращая внимания на другие важные свойства информации.

Термин «электронная информация» расширяет количество устройств, в которых может находиться информация. Таким образом, аналоговый телевизор, микроволновую печь и т.п. тоже можно отнести к устройствам, в которых может обращаться электронная информация. Однако совершить неправомерный доступ к

---

[1] *Суслопаров А.В.* Компьютерные преступления как разновидность преступлений информационного характера: дисс…. канд. юрид. наук. Красноярск, 2010. С. 10.

[2] *Гайфутдинов Р.Р.* Понятие и квалификация преступлений против безопасности компьютерной информации: дисс…. канд. юрид. наук. Казань. 2017. С.51.

ним невозможно, а также там, как правило, отсутствует охраняемая законом информация, к которой ограничили доступ.

Разделять информацию на цифровую и аналоговую тоже не совсем верно в рамках юридических наук, так как это опять вызывает зависимость определения информации от устройства, в котором она находится.

Частое изменение нормативно-правовых актов в отношении охраняемой законом информации характеризуется тем, что изменения запаздывают или решают проблему лишь частично, в результате чего в законодательстве множатся правовые коллизии[1].

Технический прогресс обгоняет теоретическое осмысление происходящего в области создания и применения информационных технологий. В связи с этим многие противоправные посягательства просто выпадают за пределы действия Уголовного Кодекса Российской Федерации.

На наш взгляд, необходимо отказаться от определения охраняемой законом информации через место ее нахождения, зависимость от какого-либо технического устройства, способа обработки.

Понятие «охраняемая законом информация» применяемая в рамках науки уголовного права, за нарушения оборота которой предусмотрена уголовная ответственность, включат в себя объем понятий «аналоговая информация», «цифровая информация», «компьютерная информация», «электронная информация» и другие виды информации, то есть является родовым по отношению к ним. Синонимия таких понятий, как «цифровая», «компьютерная» и «электронная» информация, ведет к неоправданному сужению признаков объективной стороны ст. 272 УК РФ. Они отражают только специфическую форму охраняемой законом информации, такой позиции придерживается ряд ученых[2]. Форма информации, охраняемой законом, может поменяться и из-за

---

[1] Васильев В. А. Проблемы развития законодательства в сфере борьбы с киберпреступностью // crime-research.ru. URL: http://crime-research.ru/articles/vasil06.

[2] *Гаврилов В.М.* Противодействие преступлениям, совершаемым в сфере компьютерной и мобильной коммуникации организованными преступными группами. Саратов: Саратовский Центр

цифровых устройств, где данные записаны в виде двоичного кода, она может быть переведена в удобную для восприятия человеком форму: текст, рисунок, звук, видео, которая будет отображена не в цифровом носителе информации. Таким образом свои свойства информация не потеряет (охраняемость, ограничение доступа и др.), а лишь поменяет форму отображения.

Между тем, представление даже о месте нахождения компьютерной информации весьма ограничено, так 75 % из опрошенных указали только на компьютер, остальные, наряду с компьютером, назвали другие устройства (телефон, планшет и т.д.). Также информация может находиться не только в компьютере и различных гаджетах, но в приборах учета электрической энергии.[1]

Информация может обладать юридическими свойствами и поэтому ее можно подвергнуть правовому регулированию. Нельзя не согласиться с мнением Н.Н. Ковалевой, которая к юридическим свойствам информации относит следующие:

1. Физическая неотчуждаемость – информацию нельзя отделить от ее носителя. Например, если человек сочинил компьютерную игру или мобильное приложение и в последующем продает их, то эта информация не исчезнет у него после совершения сделки, как если бы он продал недвижимость или автомобиль; таким образом, отчуждение информации заменяется передачей прав на ее использование. Схожую позицию занимает В.М. Быков, который считает, что информация не может существовать сама по себе, а всегда привязана к какому-либо носителю[2].

2. Обособленность – информация для включения в гражданский оборот используется в виде символов, знаков, таким образом, обособляется от производителя и существует отдельно.

по исследованию проблем организованной преступности и коррупции: Сателлит, 2009. С. 11; *Бегишев И.Р.* Указ соч. С. 10.

[1] Архив Новочеркасского городского суда Ростовской области, 2018 г., уголовное дело № 1-351/2018.

[2] *Быков В.М., Черкасов В.Н.* Новый закон о преступлениях в сфере компьютерной информации: ст.272 УК РФ // Российский судья. 2012. №5. С.15.

3. Двуединство информации и носителя заключается в том, что информация – это вещь на материальном носителе.

4. Распространяемость (тиражируемость) – возможность распространения неограниченного количества экземпляров без изменения содержания информации.

5. Организационная форма информации – документ.

6. Экземплярность – существование информации на отдельном материальном носителе, отсюда учет количества экземпляров через учет количества носителей. Важно отметить, что этими же свойствами обладает и электронная информация[1].

Вместе с тем, если информация рассматривается в виде объекта уголовно-правовой охраны, то к указанной классификации, по мнению автора, необходимо добавить еще одно свойство – охраняемость информации, то есть доступ к ней должен быть ограничен каким-либо нормативно-правовым актом. Другими словами, информация должна быть легально отнесена к сведениям, свободный доступ к которым запрещен.

В литературе встречаются предложения использовать термин «компьютерная информация ограниченного доступа».[2] Информация ограниченного доступа и охраняемая законом информация – это равнозначные понятие, однако второе имеет ряд преимуществ. Во-первых, ограничить доступ к информации может ее владелец, но она при этом она может не охраняться законом и нарушения оборота которой не повлекут уголовной ответственности. Во-вторых, указание на закон позволит отграничить охраняемую информацию от открытой информации.

В некоторых случаях информация может быть защищена лишь от копирования и распространения (например, авторским правом), но при этом будет являться открытой для доступа. Копирование и распространение информации без

---

[1] *Ковалева Н.Н.* Информационное право России // Учебное пособие. М., 2007. С. 3.

[2] *Сало И.А.* Преступные действия с компьютерной информацией ограниченного доступа: автореферат дисс… канд. юрид. наук. М., 2011. С. 9.

неправомерного доступа к ней (а если она открытая, то неправомерный доступ к ней не возможен по ее сути) не подлежит квалификации по ст. 272 УК РФ и не охраняется другими нормами Уголовного кодекса Российской Федерации в сфере оборота информации.

На наш взгляд, охраняемая законом информация ограниченного доступа как предмет преступного посягательства – это сведения, на которые распространяется режим ограниченного доступа, установленный Конституцией РФ и Федеральными законами и ограниченные владельцем информации от неправомерного доступа. Собственно говоря, можно выделить два главных свойства охраняемой законом информации:

1. Владелец информации предпринял действия по ее защите, например, установил пароль.

2. Информация подпадает под сведения ограниченного доступа, режим оборота которых регулируется федеральным законом.

Учитывая, что информация ограниченного доступа в любом ее виде охраняется законом и нахождение ее в каком конкретном устройстве на общественную опасность не влияет, нет необходимости выделять из нее отдельную категорию в виде компьютерной, электронной, цифровой информации или еще какой-либо.

Таким образом, предлагаем оставить в УК РФ понятие «охраняемая законом информация», неправомерный доступ к которой при наступлении общественно-опасных последствий будет уголовно-наказуемым деянием.

Предметом преступления в сфере обращения охраняемой законом информации, следует признавать любую информацию, которая охраняется законом, благодаря чему будет достигаться унификация и единообразие терминов и определений на законодательном уровне. Охраняемая законом информация ограниченного доступа как предмет преступного посягательства – это сведения, на которые распространяется режим ограниченного доступа, установленный Конституцией РФ и Федеральными законами, и ограниченные владельцем

информации от неправомерного доступа.

Также необходимо отметить, что информация может быть не ограничена от доступа, но на нее может распространяться запрет на копирование и модификацию. Однако, такая информация не будет являться предметом уголовно-правовой охраны в силу конструкции ст. 272 УК РФ, так как наступление последствий в виде копирования, блокирования, модификации, без выполнения объективной стороны состава преступления, то есть без неправомерного доступа к информации, не образует состава преступления. В других статьях Уголовного Кодекса РФ, предусматривающих ответственность за нарушение оборота охраняемой законом информации, тоже предусмотрено, что информация должна быть ограниченного доступа и составлять какую-либо тайну.

Проблеме распространения персональных данных государство начало уделять вниманием совсем недавно. Персональные данные – это информация, позволяющая идентифицировать физическое лицо (А), свободный оборот которой создает опасность причинения вреда законным интересам личности (Б), и по поводу которой установлен правовой режим конфиденциальности (В)[1]. Примером может служить направление Роскомнадзором администрации Telegram уведомления с требованием ограничить работу ботов, позволяющих пользователям получить информацию практически о любом человеке по запросу, нарушая при этом законодательство о защите персональных данных, которое было удовлетворено в марте 2021 года. Ведомство также попросило правоохранительные органы установить причастных к распространению персональной информации лиц.

Такие боты существуют несколько лет, сейчас их несколько десятков. Они собирают информацию из различных утекших и открытых баз данных и консолидируют ее (базы данных ГИБДД, базы данных Росреестра, базы данных налоговых органов и др.). Эксперты оценивают прибыль подобных ботов в 200

---

[1] *Гутник С.И.* Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: автореферат дисс… канд. юрид. наук. – Владивосток., 2017. – С. 9.

млн рублей в год[1].

Понятие информации, нарушение оборота которой запрещено, закреплено в ФЗ № 149-ФЗ, однако перечень такой информации до сих пор не установлен. В этой связи надо отметить, что информацию можно классифицировать по виду нормативно-правового акта, относящего информацию к сведениям ограниченного доступа (см. приложение 1).

В зависимости от места нахождения охраняемой законом информации ограниченного доступа, предлагаем разделить ее на следующие виды:

1. Электронный почтовый ящик. Преступники используют его для получения доступа к кошелькам в электронных платежных системах, а также для получения доступа к персональной учетной записи на каком-либо интернет-сайте, либо доступа к учетной записи социальных сетей в сети Интернет.

2. Интернет-сайт. Обычно это популярные ресурсы в сети Интернет, преимущественно финансовые проекты.

3. Профиль в социальных сетях. В ходе анализа уголовных дел было выявлено, что информация, находящаяся в социальной сети («В контакте», «Одноклассники» и др.) чаще становится объектом преступного посягательства по мотивам мести, из хулиганских побуждений, нежели из корыстных побуждений. И это отделяет ее из остальных видов.

4. Счет в электронных платежных системах (Qiwi-кошелек, Яндекс.Деньги, Perfect Money и др.).

5. База данных (абонентов операторов связи, ГИБДД и др.).

6. Локальная сеть. Возможность доступа к ресурсам (программы, файлы, папки и др.) всех соединенных между собой посредством кабелей (телефонных линий, радиоканалов) компьютеров.

7. Компьютер. Получив доступ к компьютеру, у злоумышленника появляется возможность получить неправомерный доступ к вышеперечисленной

---

[1] РКН потребовал заблокировать телеграм-боты по «пробиву данных» граждан // interfax.ru – URL: https://www.interfax.ru/russia/755038.

информации.

8. Средства мобильной связи (как правило, с операционной системой Android, в силу ее обширной распространенности).

Также наряду с информацией, которая относится законом к охраняемой, назрела необходимость во введении еще одной категории информации, охраняемой законом – пользовательской информации. Данная категория информации появилась относительно недавно и в уголовно-правовом и криминологическом контексте мало исследована, чаще пользовательская информация встречается в научных трудах в рамках рассмотрения проблем по безопасности и защиты информации[1].

Понятие «права человека» впервые можно встретить во французской «Декларации прав человека», принятой в 1789 г. Также идеи прирожденных прав были изложены в английской «Великой хартии вольностей (1215), английском Билле о правах (1689) и американском Билле о правах (1791). Однако мир сегодня стремительно меняется, вместе с этим меняется объем прав человека, предоставляемых государством. Мы живем во времена цифровой революции. Наряду с основными правами человека появляются и цифровые права. К основным правам человека, которые гарантированы Конституцией РФ и международно-правовыми актами, принято относить право на свободу выражения мнения (свобода получать и распространять информацию без вмешательства со стороны государства); право на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени; право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений и др. С

---

[1] *Новиков С.Н.* Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / под ред. В.П. Шувалова. М.: ООО «Горячая линия-Телеком», 2015. с. 128; *Борздыко И.А., Черномазов Н.М.* Применение FTP серверов для обмена и хранения пользовательской информации // Современные научные исследования и инновации. 2016. №1(57). С.233-234; *Сорокин О.Л., Сидоркина И.Г.* Анализ представления пользовательской информации в приборе «ТЕРЕМ-4» для измерения температуры ограждающих конструкций // Кибернетика и программирование. 2015. №5. С. 193-198; *Ai, H., Maiga, A. & Aimeur, E.* (2009). Privacy Protection Issues in Social Networking Sites. In Proceedings of The 7th IEEE/ACS International Conference on Computer Systems and Applications, AICCSA 2009, Rabat, Morocco, May 10-13, 2009. doi: 10.1109/AICCSA.2009.5069336;

проникновением технологий во все сферы жизни, в том числе и социальной, а также неизбежным процессом цифровизации общества, появились цифровые права[1].

Пользовательскую информацию также можно определить, как «цифровой след» – это совокупность информации, размещаемой пользователем о себе в сети Интернет[2]. Также к этому определению следует добавить иную информацию, которую пользователь сам не размещает, а которая собирается сайтами в сети Интернет и приложениями для телефонов – маршруты передвижений, биометрические данные, покупки, видеозаписи камер наблюдений и т.д.

Такого рода информация о поведении людей и действиях в сети Интернет, не попадает под закон о защите персональных данных, поскольку точно не идентифицирует человека, а только позволяет вычислить его косвенно. Таким образом, ее сбор никак не регламентирован, а пользователь никак не защищен.

Социальные сети и поисковые системы в сети Интернет собирают сведения об интересах и предпочтениях пользователей (фотографии, имена, дату рождения, адрес проживания, телефон, интересы, поисковые запросы). Эти данные необходимы для маркетинговых целей и крупные компании готовы платить деньги за цифровой портрет потребителей, чтобы эффективнее продавать свои товары и услуги. Такая деятельность не противоречит закону, однако, попадая в руки киберпреступников, данная информация может быть использована ими против пользователей этой информации.

С одной стороны, кажется, что ничего плохого в сборе данных о пользователях сети Интернет нет. Ведь благодаря этому нахождение в сети

---

[1] *Смирнова И.Г.* Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / под науч. ред. И. Г. Смирновой. М.: Юрлитинформ, 2016. 312 с.; *Родивилин И.П., Родивилина В.А.* Защита цифровых прав человека // Материалы Всероссийской научно-практической конференции «Конституция Российской Федерации и правовая политика на современном этапе». 2019. С. 104-110; *Кучеров И.И.* Криптовалюта как платежное средство // Финансовое право. 2018. №7. С. 3-6.

[2] *Бояркина Л.А., Бояркин В.В.* Цифровой след и цифровая тень как производные персональных данных // Сборники конференций НИЦ Социосфера. – Прага: Vedecko vydavatelske centrum Sociosfera-CZ s.r.o., – 2016. – № 62. – С. 71–78.

Интернет становится интереснее и полезнее: пользователю советуют то, что, скорее всего, его заинтересует, однако при плохой защите персональные данных со стороны корпораций, может произойти утечка указанной информации.

Пользовательские данные могут попасть в базы данных, даже если пользователь использует кнопочный телефон. Некоторые приложения при установке получают доступ к списку контактов, например, «GetContact». Таким образом, пользователь «сливает» не только свои данные, но и контакты всех людей, сохраненных в телефонной книге. Следует указать, что использование данной программы запрещено в Республике Казахстан на законодательном уровне.

Также сайтам и приложениям известно местоположение пользователя. С помощью программ можно отслеживать и фиксировать местоположение, а уже на основе этих данных предлагать персонализированную рекламу.

Компания «Google» хранит не только поисковые запросы пользователя, но и список статей, которые он прочитал, профили людей в социальных сетях, страницы которых посещал пользователь. Данные о контактах, планы в календаре, будильники, приложения, которыми пользуются люди, их музыкальные предпочтения и даже уровень заряда аккумулятора – ещё один перечень данных, которые Google собирает для показа более релевантной рекламы. Если пользователь хотя бы раз использовал фразу «Окей, Google» для составления поискового запроса, то его голосовые команды для управления смартфоном, а также голосовые поисковые запросы сохранены на серверах Google.

Высока вероятность того, что фотографии и видео пользователя смартфоном на Android, хранятся в облачном хранилище Google, а пользователь такого смартфона об этом даже не знает, потому что автозагрузка могла быть включена по умолчанию. Удаление приложения Google Photo с устройства не исправит ситуацию. Все фотографии пользователя продолжат «улетать» в «облако» и в случае утечки данных могут оказаться в открытом доступе.

В некоторых смартфонах уже используются технологии по их разблокировке с использованием лица пользователя или по отпечатку пальца. Скоро к этому списку авторизации может добавиться и голос. Недавно системы распознавания лиц запустили такие социальные сети как «Facebook», «ВКонтакте», «Одноклассники»[1]. Работает такая система с использованием нейронных сетей, которые идеально подходят для распознавания образов. Эта система позволяет отмечать пользователей на фотографиях, выкладываемых в социальную сеть. При утечке подобного рода информации, злоумышленники смогут создать фотографию или смонтировать видеоролик с участием пользователя с непристойным содержанием. Тому пример: недавняя история с программным продуктом «Deepfakes»[2], который позволяет создавать видеофайлы с порнографическим изображением, при этом добавляя любые лица.

Общественная опасность неправомерного доступа к пользовательской информации близка по своей сути к неправомерному доступу к персональным данным и в связи с отсутствием закона, предусматривающего ее охрану, предлагается признавать пользовательскую информацию предметом уголовно-правовой охраны и включить соответствующую норму в закон ФЗ «О персональных данных»[3] (далее – ФЗ № 152-ФЗ). Под пользовательской информацией следует понимать совокупность информации, собираемой о пользователях в сети Интернет. К такой информации могут относиться маршруты передвижений, биометрические данные, покупки, видеозаписи камер наблюдений, сведения об интересах и предпочтениях пользователей (фотографии, имена, дату рождения, адрес проживания, телефон, интересы, поисковые запросы).

---

[1] Зачем в социальных сетях система распознавания лиц [электронный ресурс] // gazeta.ru. URL: https://www.gazeta.ru/tech/2018/03/10/11675389/face_recognition.shtml.

[2] *Сулейманов С.* Deepfakes: порно, в которое нейросеть добавляет лица знаменитостей. Его запрещают все крупные сервисы, даже PornHub // Медуза. 2018 // URL: https://meduza.io/feature/2018/02/07/deepfakes-porno-v-kotoroe-neyroset-dobavlyaet-litsa-znamenitostey-ego-zapreschayut-vse-krupnye-servisy-dazhe-pornhub.

[3] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: в ред. Федерального закона от 27 декабря 2019 г. № 480-ФЗ // Собрание законодательства Российской Федерации. 2006. № 31. Ст. 3451.

Ввиду того, что пользовательская информация стала разновидностью информации ограниченного доступа, необходимо включить ее в ФЗ № 152-ФЗ. К пользовательской информации следует относить фотографии, ФИО, дату рождения, адрес проживания, телефон, интересы, поисковые запросы.

Подводя итог, следует подчеркнуть, что охраняемая законом информация в любом ее виде, независимо от типа носителя и способа обработки и хранения, должна охраняться, нет необходимости выделять из нее отдельную категорию в виде компьютерной, электронной или цифровой информации.

§ 2. Общая характеристика преступлений в сфере обращения охраняемой законом информации, их понятие и виды

В силу своей распространенности в обществе, информация все чаще становится предметом преступных посягательств и возникает необходимость в ее уголовно-правовой охране. На сегодняшний день можно сказать, что существует прямая зависимость роста преступлений в сфере обращения охраняемой законом информации от увеличения общего количества пользователей интернет-пространства. В этой связи нужно отметить, что подобного рода преступления обусловлены появлением нового предмета преступного посягательства – охраняемой законом информации.

Для предупреждения преступлений в сфере обращения охраняемой законом информации необходимо осмыслить данное явление. С момента введения гл. 28 в УК РФ, которая предусмотрела ответственность за преступления в сфере компьютерной информации, в научном сообществе ведутся споры относительно понятийного аппарата преступлений в указанной сфере.

В научных трудах предпринято большое количество попыток дать понятие преступлениям в сфере компьютерной информации. Несмотря на наличие положительных моментов в каждой из проанализированных дефиниций, ни одна

из них, по нашему мнению, в полной мере не отражает сущности указанного явления.

Ряд авторов придерживаются той позиции, что под преступлениями в сфере компьютерной информации следует понимать общественно опасные деяния, посягающие на общественные отношения, обеспечивающие безопасность оборота электронной информации[1]. По нашему мнению, определения указанных авторов включают в себя слишком большой объем признаков и неоправданно расширяют круг преступлений рассматриваемой категории. Также хочется отметить, что их работы были сделаны достаточно давно. Компьютерная техника и информатизация общества ушли с тех пор далеко вперед, и поэтому их определения устарели. При этом данные понятия определяют компьютерные преступления, которые шире понятия преступления в сфере компьютерной информации.

Другие авторы под преступлениями в сфере компьютерной информации понимают использование компьютера или ЭВМ[2]. Предложенные дефиниции содержат устаревшее понятие ЭВМ, которое уже давно исключено из УК РФ и других нормативно-правовых актов. Вместо него применяется термин «компьютер».

В.Б. Вехов понимает под компьютерными преступлениями (с точки зрения уголовно-правовой охраны) предусмотренные уголовным законом общественно

---

[1] *Маслакова Е.А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дисс…. канд. юрид. наук. Орел. 2008. С.9; *Спирина С.Г.* Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. Краснодар, 2001. С. 69; *Малыковцев М.М.* Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дисс…. канд. юрид. наук. М, 2007. С. 8; *Карпов В.С.* Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юрид. наук. Красноярск, 2002. С. 43; *Зубова М.А.* Компьютерная информация как объект уголовно-правовой охраны: дисс…. канд. юрид. наук. Казань., 2008. С. 9.

[2] *Лопатина Т.М.* Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дисс…. докт. юрид. наук. М., 2007. С. 17; *Гаухман Л. Д., Колодкин Л.М., Максимов С. В.* Уголовное право: Часть Общая. Часть Особенная: учебник. 2-е изд., перераб и доп. М., 1999. С. 652; *Старичков М.В.* Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дисс…. канд. юрид. наук. Иркутск, 2006. С.25; *Сало И.А.* Указ соч. С.9.

опасные действия, в которых машинная информация является объектом преступного посягательства[1]. В.А. Мещеряков под преступлением в сфере компьютерной информации («компьютерным» преступлением) понимает «запрещенное уголовным законом общественно опасное деяние (действие или бездействие), направленное против информации, представленной в особом (машинном) виде, принадлежащей государству, юридическому или физическому лицу, а также против установленного государством или ее собственником порядка создания (приобретения), использования и уничтожения, если оно причинило или представляло реальную угрозу причинения ущерба законному владельцу информации или автоматизированной системы, в которой эта информация генерируется (создается), обрабатывается, передается и уничтожается, или повлекло иные опасные последствия»[2]. В предложенных определениях также содержится устаревшее понятие «машинная информация», которое было заменено введением термина «компьютерная информация».

О.М. Сафонов под преступлениями, совершаемыми с использованием компьютерных технологий, понимает запрещенные уголовным законом умышленные деяния, причиняющие вред общественным отношениям в сфере безопасности компьютерных систем или создающие угрозу причинения такого вреда[3]. Этим высказыванием автор допускает некоторую некорректность в определениях, когда относит к таким деяниям следующие составы преступлений: ч. 1 ст. 171.2, ч. 1 ст. 185.3, п. «б» ч. 2 ст. 228.1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242.1 УК РФ) ст.159.3, ст.159.6 УК РФ. Ведь считается, что при совершении указанных преступлений вред наносится общественным отношениям в сфере экономической деятельности, незаконного оборота наркотических средств,

---

[1] *Вехов В.Б.* Компьютерные преступления: Способы совершения. Методики расследования. М., 1996. С. 23.

[2] *Мещеряков В.А.* Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук. Воронеж, 2001. С. 43.

[3] *Сафронов О.М.* Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дисс…. канд. юрид. наук. М., 2015. С. 12.

порнографических материалов, в том числе с изображением несовершеннолетних, а вовсе не безопасности компьютерных систем.

Исходя из вышеизложенных мнений, можно сделать вывод, что в научной среде отсутствует единый подход в определении понятия преступления в сфере компьютерной информации, отсутствует единая терминология, а также сложилось два основных подхода к определению компьютерной информации: через способ обработки указанной информации и через форму ее представления.

Также в большинстве случаев дефиниции преступлений в сфере компьютерной информации содержат устаревшую терминологию (ЭВМ, машинная информация) и не оперируют современной терминологией, применяемой в науке уголовного права и смежных ему отраслей права, таких как уголовный процесс, криминалистика и т.п. Также в рассмотренных определениях указаны общественные отношения, относящиеся к киберпреступлениям, то есть преступлениям в сфере компьютерной информации в широком смысле.

Представляется, что наиболее точно сущностную характеристику указанных деяний отражает их определение как преступлений в сфере обращения охраняемой информации, под которыми следует понимать виновно совершенные общественно опасные деяния, посягающее на общественные отношения, возникающие по поводу охраны информации ограниченного доступа. Такое определение обуславливается тем, что Уголовный кодекс Российской Федерации должен охранять общественные отношения в сфере обращения информации ограниченного доступа, а объект уголовно-правовой охраны не должен ограничиваться только компьютерной информацией. Принимая во внимание, что охраняемая законом информация может быть зафиксирована на цифровом носителе, может размещаться в информационно-телекоммуникационных сетях, а также на бумажном носителе, нет необходимости специально выделять в отдельную группу общественные отношения, возникающие в сфере обращения охраняемой законом информации.

Существуют различные классификации преступлений в сфере обращения охраняемой законом информации. Критериями таких классификаций выступают компьютер как предметом преступного посягательства[1]; мотивы совершения преступлений[2], виды субъектов, в том числе по их отношению к компьютерной информации, на которую направлены преступные посягательства[3]; тяжесть последствий, наступивших в результате их совершения[4] и т.д.

Названные классификации, несомненно, имеют большое научное и прикладное значение. Однако, поскольку преступления в сфере обращения охраняемой законом информации характеризуются разнообразием способов совершения, то в настоящий момент назрела необходимость в совершенствовании их классификации.

Способам совершения преступлений в сфере обращения охраняемой законом информации уделялось достаточное внимание со стороны ученых[5]. Однако большинство описанных способов потеряли свою актуальность в связи с развитием новых информационных технологий. Более того, сходные по способу совершения и непосредственному объекту преступления могут повлечь разные последствия. В связи с этим представляется целесообразным систематизировать преступления в сфере обращения охраняемой законом информации в зависимости от способа совершения преступного деяния. Тогда преступления в сфере обращения охраняемой законом информации можно разделить на следующие группы.

---

[1] *Ефремова М.А*. Указ. соч. С. 365.
[2] *Батурин Ю. М.* Проблемы компьютерного права. М., 1991. С. 129.
[3] *Айков Д., Сейгер К., Фонстрох У.* Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями. М., 1999. С. 91.
[4] *Старичков М.В.* Указ. соч. С.25.
[5] См. *Шахрай С.С.* К вопросу о способах совершения преступлений в сфере компьютерной информации // Вестник экономической безопасности. 2009. № 10. С. 98–102; *Будаковский Д.С.* Указ. соч. С. 2–4; *Коломинов В.В.* О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. 2015. № 3. С. 145–149; *Вехов В.Б.* Указ. соч. 182 с.; *Гаджиев М.С.* Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук. Махачкала, 2004. С. 70–71; *Рогозин В.Ю.* Изменения в криминалистических характеристиках преступников в сфере высоких технологий // Расследование преступлений: проблемы и пути их решения. 2015. № 1 (7). С. 56–58.

1. Использование вредоносных компьютерных программ для мобильных телефонов. С целью получения неправомерного доступа к информации, злоумышленники разрабатывают специальный интернет-ресурс, на котором осуществляется управление «зараженными» устройствами. На протяжении нескольких лет в Российской Федерации этот способ совершения преступлений в сфере обращения охраняемой законом информации является самым распространённым. Необходимо обратить внимание на тот факт, что эта группа преступлений составляет самую высокую долю в структуре нераскрытых преступлений. В ходе экспертного опроса, установлено, что доля нераскрытых преступлений составляет 96 %. Опрошенные респонденты в качестве основной причины такой тенденции указали на то обстоятельство, что злоумышленники находятся в других субъектах Российской Федерации или за границей, в связи с чем их поиск и привлечение к уголовной ответственности представляется затруднительными. В случае установления преступной группы, далеко не всегда удается выявить всех ее участников.

2. Использование вредоносных компьютерных программ для неправомерного доступа к компьютерной технике (персональный компьютер, мобильный компьютер и т.п.). Рассылка вредоносных программ по электронной почте с целью заражения компьютера и получения доступа к нему.

В отличие от рассмотренной выше группы преступлений, подобного рода деяния могут совершаться как преступниками-одиночками, обладающими необходимыми знаниями в программировании, так и группой лиц.

3. Неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам.

Совершается преступниками одиночками, не имеющими образования в информационной сфере. В большинстве случаев совершаются из корыстной заинтересованности, в редких случаях, с целью проверить свои навыки.

4. Кардинг – похищение реквизитов, идентифицирующих пользователей в сети Интернет как владельцев банковских кредитных карт, с их возможным

последующим использованием для совершения незаконных финансовых операций (покупка товаров либо отмывание денег)[1]. Последнее время набирает популярность Вэб-кардинг, то есть хищение денежных средств со счетов платежных карт, виртуальных счетов, криптовалюты с использованием сети Интернет. Низкий уровень взаимодействия между правоохранительными органами различных государств затрудняет процесс противодействия Вэб-кардингу.

Для правильного анализа и поиска решений проблемных вопросов требуется иметь представление о сущности вэб-кардинга. Вэб-кардинг отличается от «реального» кардинга тем, что операции по хищению денежных средств совершаются через сеть Интернет. Таким образом, злоумышленнику достаточно иметь компьютерное устройство, имеющее выход в глобальную сеть и необходимое количество знаний. Данное обстоятельство делает этот вид противоправного деяния очень доступным. Облегчает этот процесс наличие специальных интернет-ресурсов, на которых происходит общение кардеров, а также продажа и покупка реквизитов платежных карт и электронных счетов. Купив сведения о реквизитах платежных карт или используя личные преступные навыки (например, использование фишинга – «компьютерного преступления, мошенничества, основанное на принципах социального инжиниринга, практически точная копия сайта выбранного банка»[2], использование порно-сайта[3] и т.п.), кардер получает возможность совершить хищение денежных средств. Существует множество различных способов подобного хищения, такие как «карж» (покупка товаров в интернет-магазине), покупка авиабилетов, оплата каких-либо услуг через сеть Интернет, например, штрафов ГИБДД, чипдампинг (умышленное проигрывание в онлайн-играх, как правило, онлайн-покер).

---

[1] *Сачков Д.И., Смирнова И.Г.* Обеспечение информационной безопасности в органах власти: учебное пособие. Иркутск, 2015. С. 29.

[2] Что такое Фишинг // kaspersky.ru. URL: https://support.kaspersky.ru/viruses/general/2313.

[3] В Евросоюзе, США, Японии и в некоторых других странах посещение порно-сайтов является платным, для просмотра контента необходимо произвести оплату, для чего в специальной графе вводятся данные платежной карты.

Данный вид преступной деятельности является новым для уголовного законодательства России и в официальной статистике представлен не слишком высокими показателями, хотя рост этой деятельности наблюдается. Важно учесть, что, особенности функционирования сети Интернет «требуют, чтобы на решение вопросов кибербезопасности были обращены совместные усилия различных субъектов, как государственных, так и частных»[1].

Государство обратило внимание на проблему неправомерного оборота средств платежей лишь в 2015 году, с принятием изменений в ст. 187 УК РФ. Согласно внесённым изменениям, уголовно-наказуемыми стали не только деяния по изготовлению и сбыту поддельных пластиковых карт, но и по их хранению с целью использования. Необходимо также обратить внимание на тот факт, что объектами преступного посягательства теперь служат не только пластиковые платежные карты, но и распоряжения о переводе денежных средств, документы или средства оплаты, электронные средства. Состав преступления является формальным, так как наступления общественно опасных последствий не требуется.

Следует отметить, что кардинг, как правило, образует совокупность преступлений, хотя правоохранительные органы нередко квалифицируют указанные действия не по всем совершенным деяниям, что влечет недооценку общественной опасности содеянного. Важно учесть, что если кардер получает доступ к информации, находящейся в информационной системе и копирует, удаляет или модифицирует электронную информацию, но хищения денежных средств не происходит, то выполняется объективная сторона ст. 272 УК РФ. При вводе информации о реквизитах платежных карт, образуется состав преступления, квалифицируемый по ст. 159.6 УК РФ, то есть хищение путем ввода компьютерной информации.

---

[1] *Huey L.* Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime / L. Huey, J. Nhan, R. Broll // Criminology and Criminal Justice. 2013. Vol. 13, № 1. P. 81–97. DOI: 10.1177/1748895812448086.

Вместе с тем, как показывают результаты проведенного экспертного опроса, вызывает серьезные трудности выявление и расследование кардерства. Большинство респондентов (94 %) указали на сложности, возникающие в процессе выявления указанных деяний. Причем в подавляющем большинстве случаев (85 %) они обусловливаются отсутствием потерпевшего лица на территории России, либо на то, что злоумышленник находится в другом субъекте Российской Федерации или за границей. Также 89 % респондентов указали, что в настоящее время правоохранительные органы концентрируют основные усилия на противодействии единичным случаям кардинга. При этом наиболее общественно опасным формам преступного поведения – межрегиональной и международной преступности, – не уделяется достаточного внимания, и выявить такое преступление достаточно сложно, ведь факт хищения фиксируется в правоохранительных органах иностранного государства. Некоторые государства передают информацию о подобных фактах по каналам Интерпола, но большинство этого не делает. В ходе опроса 30 сотрудников национального бюро Интерпола, сделан вывод о том, что одним из немногих государств, которые сообщают о таких ситуациях в правоохранительные органы России по каналам Интерпола является ФРГ, однако это происходит в форме направления информации и не содержит всех необходимых документов, требуемых для решения вопроса о возбуждении уголовного дела в рамках уголовно-процессуального законодательства Российской Федерации.

Следует отметить, что вэб-кардинг тесно связан с использованием вредоносных компьютерных программ.

Так в Иркутской области была выявлена группа лиц, занимавшаяся распространением вредоносных компьютерных программ для операционной системы Android, с целью последующего хищения денежных средств со счетов платежных карт. Суд квалифицировал их действия по признакам составов преступлений, предусмотренных п.п. «а», «в» ч. 2 ст. 158, ч. 3 ст. 183, ч. 2 ст. 272,

ч. 2 ст. 273 УК РФ[1]. Участники группы на интернет-ресурсе, специализирующемся на хищениях денежных средств со счетов платежных карт, узнали о необычном способе хищения денежных средств при помощи вредоносного программного обеспечения для операционной системы Android. Схема хищения заключалась в следующем: участники группы разработали интернет-ресурс, на котором осуществлялось управление зараженными устройствами. Сайт размещался на так называемых «абузоустойчивых» хостингах (от англ. abuse – злоупотребление) в странах, которые неохотно выдают информацию правоохранительным органам. При установке приложений, скачивании файлов из MMC-сообщений происходило заражение телефонного аппарата вредоносной программой, и злоумышленники получали доступ к реквизитам платежных карт, которые сами владельцы зараженных телефонных аппаратов направляли им, ничего не подозревая о противоправности их действий. На экране телефонного аппарата жертвы отображалось сообщение о том, что необходимо заново ввести данные платежного средства в магазине приложений «Play Маркет».

5. Скимминг. Скиммер – это устройство, которое прикрепляется к банкомату и считывает информацию с пластиковой карты[2].

6. Ddos-атака.

Преступления в сфере обращения охраняемой законом информации базируются на стремительном развитии и использовании информационных технологий и характеризуются постоянным наращиванием и совершенствованием способов их совершения[3]. В этой связи, хотелось бы осветить относительно новую разновидность преступлений в сфере обращения охраняемой законом информации, набирающую рост в современной законодательной практике и

---

[1] Архив Октябрьского районного суда г. Иркутска, 2016 г., уголовное дело № 1-50/2016.

[2] *Протасевич А.А., Зверянская Л.П.* Способы совершения преступлений с использованием поддельных банковских карт // Актуальные проблемы теории и практики правотворчества и правоприменения (к 20-летию юридического образования в БГУЭП). 2015. С. 58.

[3] *Репецкая А.Л., Родивилин И.П.* Незаконное ограничение доступа к компьютерной информации в сети Интернет: уголовно правовой аспект // Библиотека уголовного права и криминологии. 2016. № 3(15). С. 80.

получившие название «DdoS-атака» (атака типа «отказ в обслуживании», от англ. Denial of Service), то есть атака на вычислительную систему с целью довести её до отказа, или другими словами создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Такие атаки могут быть совершены как на популярные интернет-ресурсы, так и на сайты конкурентов. По оценкам компании Group-IB, одним из основных источников доходов хакеров стали атаки на сайты при помощи фиктивных запросов (DdoS-атаки), при этом оборот незаконного рынка составляет 109,8 млн. долларов[1].

Наиболее распространенной DdoS-атакой является атака типа HTTP-flood. В ее основе лежит отправка HTTP-запросов GET. Данная flood-атака также может быть направлена на уязвимые места сервера, занятые выполнением ресурсоемких задач. В результате сервер становится неспособным к обработке запросов, так как не успевает обрабатывать запросы, посредством которых его атакуют[2].

Приведенная выше классификация преступлений в сфере обращения охраняемой законом информации отражает современную картину совершения указанных преступлений, так как содержит в себе практически все известные способы, реализованные злоумышленниками в период с 2010 по 2020 годы.

Таким образом, можно сделать следующие выводы:

1. Под преступлениями в сфере обращения охраняемой законом информации следует понимать виновно совершенное общественно опасное деяние, посягающее на общественные отношения, возникающие по поводу охраны информации ограниченного доступа.

2. Признаками такой информации является то, что ее владелец предпринял действия по защите данной информации; и она подпадает под

---

[1] Оценка объемов рынка киберпреступности в РФ // group-ib.ru. URL: http://report2013.group-ib.ru.

[2] *Остапенко Г.А., Бурса М.В., Иванкин Е.Ф.* Аналитическое моделирование процесса реализации Ddos-атаки типа HTTP-flood. // Информационная безопасность. 2013. № 1. С. 107–110.

сведения ограниченного доступа, режим оборота которых регулируется Конституцией РФ или федеральными законами

3. Преступления в сфере обращения охраняемой законом информации можно классифицировать в зависимости от способа совершения противоправного деяния. При этом выделяются следующие группы: использование вредоносных компьютерных программ для мобильных телефонов, неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам, кардинг, скимминг, ddos-атака.

ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ОХРАНЯЕМОЙ ЗАКОНОМ ИНФОРМАЦИИ

§ 1. Юридический анализ основных составов преступлений в сфере обращения охраняемой законом информации

Проникнуть в частную жизнь стало настолько просто, что закон уже с трудом определяет ее границы. Чтобы сохранить в тайне информацию уже недостаточно принимать элементарные меры предосторожности. Научно-технический прогресс принес с собой технологии, представляющие возможности для сбора, анализа и распространения охраняемой законом информации. Для борьбы с подобного рода противоправными действиями необходимо дать юридический анализ преступлениям в сфере обращения охраняемой законом информации.

В ряде рассматриваемых преступлений у правоприменителей и ученых имеются сложности при определении объекта преступления. Одни авторы считают, что под общим родовым объектом преступлений в сфере обращения охраняемой законом информации следует понимать «общественные отношения, связанные с использованием компьютерной информации»[1]. Другие, наряду с общественными отношениями, связанными с информацией, под объектом преступлений в сфере обращения охраняемой законом информации выделяют личность, сферу экономики, общественную безопасность и общественный порядок, сферу функционирования государства, безопасность человечества»[2]. Третьи выделяют в этом составе, наряду с основным, факультативный непосредственный объект.

---

[1] *Быков В.М., Черкасов В.Н.* Новая редакция ст. 274 УК // Законность. 2012. № 2. С. 28

[2] *Герасимова О.А.* Особенности преступлений в сфере компьютерной информации // Вестник ТГУ. 2007. № 12 (56). С. 327–330.

Также существует мнение, что «защищаемым объектом преступлений в сфере компьютерной информации являются общественные отношения, обеспечивающие информационную безопасность внутри государства и самого государства Российского»[1]. Исходя из данного подхода, следует, что совершаемые с территории России действия, направленные на защищаемую информацию в других странах через международные компьютерные сети, не могут быть признаны преступными. Такое толкование уголовного закона создает условия для безнаказанности хакеров, затрудняет международную интеграцию правоохранительных органов России и других стран в защите информации ограниченного доступа, поскольку в определенных случаях исключает возможность для осуществления такой работы на законных основаниях.

Вклад перечисленных ученых в разработку проблем значителен, тем не менее, нельзя не признавать того, что приведенные выше определения нуждаются в доработке, а некоторые вообще не соответствуют современным реалиям ввиду отсутствия в нормативных документах понятия ЭВМ, машинный носитель.

С учетом места гл. 28 УК РФ в системе Особенной части УК РФ (Раздел IX) можно сделать вывод о том, что под общим объектом преступлений в сфере обращения охраняемой законом информации следует понимать общественные отношения, обеспечивающие информационную безопасность. Учитывая трансграничный характер преступлений в сфере обращения охраняемой законом информации, указанное определение следует дополнить территориальной характеристикой – как на территории Российской Федерации, так и за ее пределами.

Неправомерный доступ к охраняемой законом информации зачастую имеет схожий предмет преступного посягательства – охраняемую законом информацию и становится способом совершения иных преступлений, таких как нарушений тайны переписки, личной или семейной тайны, собирание сведений,

---

[1] *Чирков П.А.* Об объекте преступлений в сфере компьютерной информации в российском уголовном праве // Правовые вопросы связи. 2012. № 1. С. 23.

составляющих банковскую или коммерческую тайну. Указанные преступления имеют другой основной непосредственный объект, а в диспозиции соответствующей статьи Особенной части УК РФ отсутствует указание на такой способ совершения преступления. Однако практика показывает, что неправомерный доступ к информации зачастую рассматривается как способ совершения иного преступления и не выделяет реальную совокупность преступления[1], что, по нашему мнению, влечет недооценку общественной опасности содеянного.

В частности, в чем заключается и в чем выражается неправомерность доступа к охраняемой законом информации? Доступ к информации можно разделить на 2 группы:

1. доступ с использованием методов обхода средств защиты информации;

2. доступ в систему, хотя и правомерный, но осуществляемый неправомерно.

Исходя из изложенного, предлагаем под неправомерным доступом к охраняемой законом информации понимать возможность воздействия на информацию лицом, не имеющим легального права на ознакомление с ней, а также лицом, хотя и имеющим право на правомерный доступ к информации, но использующим это право в нарушение правил доступа к информации.

Субъект преступления в сфере обращения охраняемой законом информации практически не вызывает трудностей при квалификации – это физическое вменяемое лицо, достигшее возраста 16 лет.

В ходе анкетирования сотрудников правоохранительных органов, не выявлено ни одного случая, когда лица, совершающие преступления указанной категории признавались невменяемыми. На наш взгляд это обусловлено тем, что выполнение действий, связанных с нарушением целостности информации, связано с

---

[1] Архив Свердловского районного суда г. Белгорода, 2012 г., уголовное дело № 1-73/2012; архив Шебалинского районного суда Республики Алтай, 2013 г., уголовное дело № 1-6/2013; архив Рузского районного суда Московской области, 2015 г., уголовное дело № 1-49/2015; архив Автозаводского районного суда г. Тольятти, 2016 г., уголовное дело № 1-834/2016; архив Кировского районного суда г. Омска, 2016 г., уголовное дело № 1-363/2016.

определенным интеллектуальным уровнем и при психическом заболевании или ином болезненном состоянии психики практически невозможно совершить указанные действия.

Преступления в сфере обращения охраняемой законом информации могут быть совершены как с прямым, так и косвенным умыслом, за исключением предусмотренных ст. 274, 274[1] УК РФ, которые могут быть совершены как умышленно, так и по неосторожности. Однако, в юридической литературе встречается мнение о том, что такие преступления совершаются только в форме умысла[1].

С учетом места гл. 28 УК РФ в системе Особенной части УК РФ (Раздел IX) можно сделать вывод о том, что под родовым объектом преступлений в сфере обращения охраняемой законом информации следует понимать общественные отношения, обеспечивающие информационную безопасность. Учитывая трансграничный характер преступлений в сфере обращения охраняемой законом информации, их определение следует дополнить территориальной характеристикой – как на территории Российской Федерации, так и за ее пределами.

Другая проблема квалификации преступлений в сфере обращения охраняемой законом информации связана с их объективной стороной, а именно с последствиями, выражающимися в форме копирования, блокирования и модификации информации.

Преступления в сфере компьютерной информации по своей конструкции относятся к материальным составам, то есть в результате совершения противоправного действия обязательно должны наступить общественно-опасные последствия, выражающиеся в уничтожении, блокировании, модификации, копировании компьютерной информации. В Уголовном Кодексе Российской Федерации не закреплены дефиниции указанных последствий, между тем они вызывают у правоприменителей множество вопросов. В ходе анализа материалов доследственных проверок, по которым вынесены постановления об отказе в

---

[1] *Малыковцев М.М.* Указ. соч. С. 170.

возбуждении уголовного дела, было установлено, что основаниями отказа в возбуждении уголовного дела часто служит формулировка: отсутствие общественно опасных последствий в виде блокирования, модификации, уничтожения компьютерной информации.

Понятие «блокирование персональных данных» дано в ФЗ № 152-ФЗ, под которым понимается временное прекращение обработки персональных данных (за исключением случаев, если обработка необходима для уточнения персональных данных). Из этого определения следует, что под блокированием охраняемой законом информации ограниченного доступа понимается временное прекращение каких-либо действий со стороны владельцев этой информации.

В словарях под модификацией понимается любое видоизменение, преобразование чего-либо, характеризующееся появлением новых свойств[1], перемена[2], видоизменения[3]. Эти же свойства можно применить к компьютерной информации. Следует отличать неправомерную модификацию от правомерной. Согласно мнению М.М. Быкова и В.Н. Черкасова, «от несанкционированной модификации следует отличать внесение изменений, которые направлены исключительно на адаптацию информации, т.е. внесение изменений, которые направлены на приспособление этой информации к функционированию с использованием конкретных технических средств пользователя»[4].

Следует отметить, что в ходе неправомерного доступа к информации происходит модификация метаданных, то есть информации об использовании информации. Так, В.В. Крылов справедливо полагает, что представляется ошибочным признавать в качестве последствия автоматическое копирование компьютерной информации, заключающееся в создании копии компьютерной

---

[1] Большой Энциклопедический словарь // academic.ru. URL: http://dic.academic.ru/dic.nsf/enc3p/200774.

[2] Словарь иностранных слов русского языка // dic.academic.ru. URL: http://dic.academic.ru/dic.nsf/dic_fwords/21984.

[3] Толковый словарь Ожегова // dic.academic.ru. URL: http://dic.academic.ru/dic.nsf/ogegova/108750.

[4] *Быков В.М., Черкасов В.Н.* Указ соч. С. 16.

информации без воли деятеля[1]. Например, при каждой сессии выхода в сеть Интернет у организации-провайдера фиксируется дата, время, выделяемый абоненту IP-адрес. Если лицо осуществит неправомерный доступ к учетной записи этого клиента, то на сервере модифицируется информация о выходе в сеть Интернет абонента, то есть метаданные. Однако эта модификация не охватывается умыслом преступника, а является следствием неправомерного доступа, так как любые действия с информацией оставляют следы на цифровых носителях информации и каждый к ней доступ изменяет (модифицирует) метаданные. Таким образом, под модификацией информации следует понимать любое видоизменение информации, за исключением изменений, происходящих автоматически при обращении с информацией (модификация метаданных).

Для уяснения смысла, вкладываемого в понятие «копирование» компьютерной информации, необходимо обратится к словарям: снимать копии с чего-нибудь[2], делать копию чего-либо[3], снимать копию с чего-нибудь[4]. А.Н. Яковлев выделяет существенный признак копирования, по его мнению, которым является получение в результате процедуры копирования нового объекта – копии, отличие местоположения копии от местоположения оригинала (пусть и в пределах одного электронного носителя информации, например, для копий файлов это будет регистрация в разных каталогах), аутентичность нового объекта оригиналу[5]. Из указанных определений следует, что создание копии информации будет признаваться копированием. По нашему мнению, неважно в каком виде эта информация будет запечатлена – в виде информации, запечатленной на компьютерном носителе либо в виде бумажной копии (например, сделанной с помощью принтера или записанной от руки). Ведь от материального носителя общественно опасные последствия, выражающие в виде копирования, не

---

[1] См.: *Крылов В.В.* Основы криминалистической теории расследования преступлений в сфере информации: дис. ... д-ра юрид. наук. М., 1998. С. 103.
[2] Толковый словарь Ушакова // academic.ru. URL: http://dic.academic.ru/dic.nsf/ushakov/840342.
[3] Современный толковый словарь русского языка Ефремовой // academic.ru. URL: http://dic.academic.ru/dic.nsf/efremova/177218.
[4] Толковый словарь Ожегова // academic.ru. URL: http://dic.academic.ru/dic.nsf/ogegova/88986.
[5] *Яковлев А.Н.* Указ. соч. С. 73.

изменятся, свойства информации также не претерпят изменений (за исключением носителя этой информации, что никак не влияет на квалификацию преступления).

В научной литературе также поднимается вопрос об исключении общественно-опасного последствия в виде копирования информации[1], что на наш взгляд не совсем верно. Любое копирование охраняемой законом информации уже нарушает защищённость и конфиденциальность информации, создает угрозу дальнейшего ее использования в иных преступных целях, например, для хищения денежных средств обладателя информации.

Понятие «уничтожение» дается в ст. 3 ФЗ № 152-ФЗ. Под ним понимаются 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. Недостаток этого определения в том, что он применим лишь к персональным данным. Следует дополнить УК РФ понятием уничтожение электронной информации, под которой следует понимать удаление электронной информации из электронного пространства, где она находилась.

Однако, в некоторых случаях, при уничтожении информации с жесткого диска компьютера, ее возможно восстановить, ведь при удалении ее в файловой системе компьютера, информация продолжает находиться, но компьютер помечает это место как свободное. В.М. Быков и Черкасов В.Н. указывают, что если информация была удалена, однако благодаря современным техническим средствам ее удалось восстановить, то следует квалифицировать действия лица в соответствие с ч.3 ст. 30 и ст. 272 УК РФ[2]. Вряд ли можно согласиться с этим мнением, ввиду того, что преступник выполнил все действия, предусмотренные объективной стороной, и преступление следует считать оконченным с момента удаления информации, а уже восстановление информации может произойти

---

[1] *Халиулилн А.И.* Неправомерное копирование как последствие преступления в сфере компьютерной информации // Российский следователь. М., 2015. № 8. С. 25.
[2] *Быков В.М., Черкасов В.Н.* Указ. соч. С. 16.

спустя некоторое время и происходит в независимости от преступника, который убежден, что уничтожил информацию.

От общественно-опасных последствий неправомерного доступа к охраняемой законом информации в виде копирования и модификации следует отграничивать модификацию и копирование метаданных, то есть информацию об использовании информации, поскольку эти действия не охватываются умыслом преступника и происходят в независимости от его действий, и не наносят вред обладателю информации. Также в УК РФ необходимо закрепить понятия блокирование, модификация, уничтожение электронной информации.

§ 2. Проблемы квалификации и отграничения от смежных составов преступлений в сфере обращения охраняемой законом информации

Преступления в сфере обращения охраняемой законом информации обладают достаточно сложной квалификацией, как уже было отмечено ранее, это связано с предметом преступления (охраняемой законом информацией) и неоднородностью объекта преступления.

Уголовный кодекс Российской Федерации предусматривает достаточно обширную систему преступлений, связанных с неправомерным оборотом охраняемой законом информации. Ее образуют посягательства, расположенные в различных разделах и главах Кодекса.

Анализ результатов исследования свидетельствует о том, что неправомерный доступ к охраняемой законом информации, создание, использование и распространение вредоносных компьютерных программ, как правило, образуют совокупность с другими преступлениями, которые посягают на другие общественные отношения: незаконное собирание и распространение информации о частной жизни лица (ст. 137 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан (ст. 138 УК РФ), разглашение тайны усыновления (ст. 155 УК РФ), незаконное

получение и разглашение банковской и коммерческой тайны (ст. 183 УК РФ), разглашение государственной тайны (ст. ст. 275, 276, 283 УК РФ), разглашение тайны предварительного расследования (ст. 310 УК РФ), разглашение сведений о мерах безопасности в отношении участников уголовного судопроизводства (ст. 311 УК РФ), разглашение сведений о мерах безопасности в отношении должностного лица правоохранительного или контролирующего органа, а также его близких (ст. 320 УК РФ) и др. Эти преступления хоть и посягают на разные общественные отношения, однако направлены на доступ в том или ином виде к охраняемой законом информации.

При этом квалификация преступлений в сфере обращения охраняемой законом информации по совокупности с другими составами преступлений вызывает некоторые трудности у правоприменителей.

Процесс накопления и оборота информации, в том числе охраняемой законом, сегодня – это одна из наиболее динамичных и быстро развивающихся сфер общественных отношений, нуждающихся в адекватном правовом регулировании. Сейчас термины «личная тайна», «коммерческая тайна», являются общеупотребительными, как в научных кругах, так и в бытовой сфере. Однако данные понятия отличаются по своей природе, их неверное употребление может создавать множество трудностей при квалификации преступлений. Следовательно, необходимо внести ясность в используемую терминологию.

Основной проблемой является определение общественных отношений, на которые посягает преступник. Ряд авторов считают, что неприкосновенность частной жизни не может рассматриваться в качестве объекта преступного посягательства при неправомерном доступе к компьютерной информации[1]. В обоснование своей позиции в качестве аргумента они приводят то обстоятельство, что сведения виновный получает в электронной форме, следовательно, признаки информации они приобретают после аналитической обработки полученных данных.

---

[1] См. *Сапранкова Т.Ю.* Проблемы систематизации преступлений, связанных с нарушением неприкосновенности частной жизни // Успехи современной науки. 2017. № 3. С. 245.

Думается, подобный подход не имеет под собой объективных оснований. Неправомерный доступ к охраняемой законом информации посягает на отношения в сфере обеспечения ее безопасности и сохранности. Однако соответствующие данные не ограничиваются лишь информацией о частной жизни[1].

Помимо этого, обращает на себя внимание и имеющая место избыточная криминализация посягательств на сохранность информации.

В целях соблюдения принципа справедливости автор предлагает декриминализировать действия по неправомерному доступу к электронной информации, если эта информация не подпадает под определение охраняемой (личная, семейная, врачебная и т.д.), то есть первую часть ст. 272 УК РФ.

Это мнение не разделяет О.М. Сафонов, который предлагает дополнить ст. 63 УК РФ отягчающим обстоятельством «совершение преступления с использованием компьютерных технологий»[2] и считает, что данное обстоятельство существенно повышает степень их общественной опасности. Однако думается, что данная позиция не обоснована ни целями уголовного права, ни здравым смыслом. Данный способ совершения преступления, по своей сути, ничем не отличается от обычного. Разница лишь в том, что в данном случае используется компьютерная техника. Например, если совершено хищение из отделения банка при помощи компьютера и сети Интернет, то разве это будет являться отягчающим обстоятельством. В данном случае может идти речь о совокупности преступлений, например, ст. ст. 158, 272, 159^6 УК РФ, в зависимости от способа совершения хищения.

В ходе анализа уголовных дел изучены обвинительные приговоры, по которым граждане были осуждены по ст. 272 УК РФ за прошивку игровых приставок, взлом электронной почты и учетных записей в социальных сетях. Представляется, что совершение указанных действий, если они не повлекли

---

[1] См. *Хурум М.А*. Преступления, связанные с получением и (или) разглашением конфиденциальной информации: криминализация, систематизация и оптимизация законодательного описания: дис. … канд. юрид. наук. Краснодар., 2019. С. 59.
[2] *Сафронов О.М.* Указ соч. – С. 9.

тяжких последствий и не причинили моральный или материальный вред, не соотносятся с принципом справедливости, согласно которому наказание и иные меры уголовно-правового характера, применяемые к лицу, совершившему преступление, должны соответствовать характеру и степени общественной опасности преступления, обстоятельствам его совершения. Описанные последствия в ст. ст. 272-274[1] УК РФ в виде копирования, блокирования, модификации и уничтожения информации не дифференцируют вред, причиненный преступлением. Например, при удалении электронного письма, в котором ведется переписка с друзьями о погоде, текущем состоянии дел и т.п. не приносит ее обладателю никакого вреда (ни морального, ни материального). А вот копирование идентификатора учетной записи и пароля для электронных платёжных систем с целью похищения денежных средств, может нанести владельцу указанной информации материальный ущерб (возможно даже в крупном размере). Или, например, копирование информации врачебного диагноза может причинить гражданину страдания, вплоть до совершения им самоубийства.

Таким образом, необходимо отграничивать преступления в сфере обращения охраняемой законом информации от административного правонарушения или перенести их в сферу уголовного проступка (если конечно закон об уголовном проступке[1] будет принят).

В.Г. Степанов-Егиянц считает необходимым введение административной ответственности за неправомерный доступ к компьютерной информации без наступления последствий, указанных в ст. 272 УК РФ[2]. Согласимся с этим мнением, с некоторыми поправками. Во-первых, считаем целесообразным привлекать к административной ответственности не только за неправомерный доступ к охраняемой законом информации, без наступления последствий в виде копирования, блокирования, модификации, но и при наступлении таковых

---

[1] Законопроект № 1112019-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с введением понятия уголовного проступка» // sozd.duma.gov.ru URL: https://sozd.duma.gov.ru/bill/1112019-7.

[2] *Степанов-Егиянц В.Г.* Объективная сторона неправомерного доступа к компьютерной информации по уголовному кодексу РФ // Библиотека криминалиста. 2013. № 5 (10). С. 47.

последствий, если эти действия не причинили моральные страдания или не совершены из корыстной заинтересованности либо мести. Несомненно, подобные нововведения усложнят процедуру привлечения к уголовной ответственности. Однако это будет способствовать повышению уровня доверия к правоохранительной системе, так как прекратится поток бессмысленных приговоров в отношении лиц, которым в силу малозначительности совершенного ими деяния возможно применить иные меры воздействия.

А также внести в кодекс Российской Федерации об административных правонарушениях следующие изменения:

1) Дополнить статьей 13.14.1 следующего содержания:

«Статья 13.14.1 «Неправомерный доступ к информации, которая ограничена федеральным законом, повлекший копирование блокирование, уничтожение, ознакомление (за исключением случаев, если разглашение такой информации влечет уголовную ответственность).

Еще одной причиной сложности квалификации преступлений в сфере обращения охраняемой законом информации является то, что диспозиции статей Особенной части УК РФ не рассматривают компьютерные технологии в качестве средств совершения других преступлений, за исключением введенной относительно недавно ст. 159^6 УК РФ «Мошенничество в сфере компьютерной информации».

По мнению М.Ю. Дворецкого, предметом преступного посягательства по ст. 159^6 УК РФ являются: 1) компьютерная информация; 2) имущество, т.е. совокупность вещей, которые находятся в собственности лица, в т.ч. включая деньги и ценные бумаги, а также имущественных прав на получение вещей или имущественного удовлетворения от других лиц. Кроме того, он считает, что в том случае, если лицо оперировало сведениями, не относящимися к компьютерной информации (в понимании уголовного закона), либо его действия не были связаны с завладением имуществом, а преследовало иные цели, (например, создание

препятствий в реализации прав собственника), уголовная ответственность по ст. 159[6] УК РФ исключается[1].

Однако, исходя из понятия хищения, которое дано в примечании 1 к ст. 158 УК РФ, предметом хищения выступает чужое имущество. Охраняемая законом информация, а именно ее ввод, удаление, блокирование, модификация в данном случае будет являться способом совершения хищения.

Все хищения характеризуются конкретным способом их совершения, который лежит в основе разграничения форм хищения (для кражи обязателен тайный способ, мошенничество характеризуется способами обмана и злоупотребления доверием и т.д.). В случае со ст. 159[6] УК РФ хищение происходит путем ввода, копирования, модификации компьютерной информации. Однако эта конструкция не вписывается в систему преступлений в сфере обращения охраняемой законом информации в силу различия предметов преступного посягательства.

Сотрудникам правоохранительных органов зачастую нелегко доказать указанные в диспозиции ст. 272 УК РФ последствия в виде уничтожения, блокирования, удаления информации. К примеру, злоумышленник осуществил неправомерный доступ к электронной информации, прочитал конфиденциальную информацию и покинул систему. Последствий не наступило, но с информацией ограниченного доступа ознакомилось третье лицо, пропустило ее через себя и может интерпретировать в своих интересах. Можно ли здесь говорить о копировании? Конечно нет, действия преступника не стали менее общественно опасны и информацию, с которой ознакомился, он может в дальнейшем использовать для совершения противоправных деяний.

Это мнение разделяет Д.А. Овсюков, который считает, что «действующее российское законодательство не в полной мере способно осуществлять защиту от несанкционированного блокирования информации в сети Интернет в связи с

---

[1] *Дворецкий М.Ю.* Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. Томск, 2013. № 8 (124). С. 407.

несовершенством существующих уголовно-правовых норм, отсутствием связи между юридическими формулировками и техническими особенностями совершения указанного вида преступлений, поэтому требует более детальной проработки»[1].

Сохранение в кэше браузера информации о посещении какого-либо ресурса не охватывается умыслом преступника, а происходит автоматически, что не подпадает под последствия, указанные в ст. 272 УК РФ.

Особую актуальность приобретает правовая регламентация оборота криптовалют, что подтверждается активным обсуждением правовых вопросов использования криптовалют среди ученых[2]. Оборот криптобирж за 2016 г. в мире увеличился с 48 до 415 млн. долл.[3], а криптовалюта получает свое применение в качестве эффективного финансового инструмента не только на рынке повседневных товаров услуг, но и на «черном» и «сером» рынках.

Предмет преступлений в сфере обращения охраняемой законом информации может отличаться от предмета аналогичных преступлений, совершаемых в материальном мире, и иметь свои особенности. Поскольку

---

[1] *Овсюков Д.А*. Блокирование информации в информационно-телекоммуникационной сети Интернет путем создания искусственной перегрузки компьютерной системы: уголовно-правовой анализ // Российский следователь. М. 2014. № 4. С. 36.

[2] *Батоев В.Б., Семенчук В.В*. Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии управления МВД России. 2017. № 2 (42). С. 9–15; *Васюков В.Ф.* Отдельные вопросы производства осмотра при расследовании преступлений, совершаемых с использованием криптовалюты // Современное уголовно-процессуальное право России - уроки истории и проблемы дальнейшего реформирования: Сб. мат-лов Междун. науч-практ. конф. К 300-летию российской полиции и 100-летию советской милиции. Орловский юридический институт МВД России имени В. В. Лукьянова. 2017. С. 83-87; Галушин П.В., *Карлов А.Л.* Сведения об операциях с криптовалютами (на примере биткойна) как доказательство по уголовному делу // Ученые записки Казанского юридического института МВД России. 2017. Т. 2. № 4. С. 90-100; *Дельцова Т.А*. Денежные суррогаты в российской федерации: прошлое, настоящее, будущее // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. 2016. № 1 (43). С. 164-166; *Простосердов М.А.* Криптовалюта как предмет хищения // Российское правосудие. 2016. № 6 (122). С. 107-111; *Симаков А.А.* Анонимность в глобальных сетях // Научный вестник Омской академии МВД России. 2017. № 2 (65). С. 62-65; *Родивилин И.П., Родивилина В.А.* Криптовалюта как объект преступления // сборник материалов международной научно-практической конференции «Деятельность правоохранительных органов современных условиях». 2018. С. 262-265.

[3] См.: *Сидоренко Э.Л*. Криптовалюта как новый юридический феномен // Общество и право. 2016. №3 (57). С. 193.

киберпространство является сферой деятельности в информационном пространстве, т.е. некой виртуальной реальностью, то такие общественно опасные деяния, как, например, хищения (ст. 159, 159.6, 160 УК РФ), не могут быть направлены на изъятие конкретных материальных предметов (бумажник, телефон, автомобиль), поскольку они просто не могут существовать в киберпространстве. Однако данные преступления могут быть направлены на другие предметы, обладающие такой же экономической значимостью, существование которых возможно в цифровой среде (безналичные и электронные денежные средства, криптовалюта).

По своей природе любая криптовалюта – это уникальное цифровое число, представленное в форме компьютерной информации. Данное число используется как денежный эквивалент: на него можно что-либо купить либо обменять на настоящие деньги, поскольку у каждой криптовалюты есть собственный курс. Однако в связи с природой криптовалюты возникает серьёзная теоретическая проблема: поскольку любая криптовалюта это информация, то может ли она являться предметом хищения, а возможен ли к ней неправомерный доступ, влекущий общественно-опасные последствия в виде копирования, блокирования, модификации?

В уголовно-правовом регулировании хищения криптовалют до 1 октября 2019 года существовал пробел. С этого времени криптовалюта законодательно отнесена к объектам гражданских прав. В связи с вышесказанным хищение криптовалюты является преступлением и подлежит квалификации с учетом иных элементов составов преступлений и может быть квалифицировано по ст. 158 УК РФ, ст. 159 УК РФ, ст. 160 УК РФ, ст. 162 УК РФ и другим имущественным преступлениям.

Однако хранится криптовалюта либо на носителе информации у самого пользователя, либо на специальном сервере и является информацией, которую можно, вопреки воле ее законного владельца, модифицировать, скопировать, удалить. Криптовалюта – распределенная, основанная на математических

принципах пиринговая виртуальная валюта с открытым исходным кодом, при использовании которой отсутствует централизованный администратор, а также соответствующие контроль и надзор (Bitcoin, LiteCoin, Ripple и др.) со стороны государственных органов или иных третьих лиц[1]. Следовательно, приобретая криптовалюту за реальные (настоящие) деньги, покупатель приобретает уникальную индивидуально определённую вещь, имеющую коммерческую ценность, то есть товар, но в виде определенного набора символов (информации). Криптовалюта – это «хорошо защищённый файл, признанный платёжной единицей… (аналог нынешнего наличного оборота)... прообраз настоящих электронных денег отдалённого будущего»[2].

Также как и доступ к учетной записи в социальной сети пользователя (например, vk.com, Instagram и др.), доступ к учетной записи, где находится криптовалюта и где ей можно распорядиться, ограничивается паролем, а также приватным ключом, который необходим для владения криптовалютой и для осуществления с ней финансовых операций. Таким образом, злоумышленник, имея пароль (который был украден или подобран с использование программного обеспечения, предназначенного для автоматизированного подбора пароля к учетным записям – брутфорс[3]), может совершить неправомерный доступ к информации, находящейся в учетной записи пользователя и скопировать данные кошелька, удалить его или модифицировать информацию. Однако, такие действия не подпадают под уголовно-наказуемое деяние, так как информация о кошельке криптовалюты в настоящий момент никаким законом не охраняется.

---

[1] Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ. URL: http://www.eurasiangroup.org/ files/FATF_docs/Virtualnye_valyuty_FATF_2014.pdf.

[2] Фатьянов А.А. Правовой анализ категории «электронные денежные средства» в российском законодательстве. Гражданское общество в России и за рубежом. 2014.№ 3. // СПС «КонсультантПлюс».

[3] Брутфорсом называется метод доступа к различным учетным записям, путем подбора логина и пароля. Еще брутфорс называют методом грубой силы. Его суть заключается в автоматизированном переборе всех допустимых комбинаций пароля к учетной записи с целью выявления правильного, является разновидностью хакерской атаки. Брутфорс – один их самых популярных методов взлома паролей учетных записей онлайн-банков, платежных системах или на вебсайтах.

Преступления в сфере обращения охраняемой законом информации в большинстве случаев образуют реальную совокупность преступлений с другими общественно-опасными деяниями, посягающими на один предмет – охраняемую законом информацию, но при этом имеют разные основные непосредственные объекты. В этой связи, верным представляется утверждение о том, что необходимо квалифицировать подобные деяния по нескольким составам Особенной части УК РФ, оценивая общественную опасность каждого преступления.

ГЛАВА 3. КРИМИНОЛОГИЧЕСКАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ОХРАНЯЕМОЙ ЗАКОНОМ ИНФОРМАЦИИ

§ 1. Состояние, структура и динамика преступлений в сфере обращения охраняемой законом информации

Активное развитие телекоммуникационных технологий способствовало вовлечению множества людей в виртуальное пространство. Сложно предстать современное общество без сети Интернет, электронной почты, мобильных мессенджеров и т.д. В списке стран с высоким уровнем совершаемых преступлений в виртуальной среде Россия занимает 1-е место и одновременно относится к группе самых незащищенных от киберугроз государств[1].

На электронный рынок платежей обратили свой взгляд как профессиональные, так и начинающие интернет-преступники. Похищение реквизитов, идентифицирующих пользователей в сети Интернет как владельцев банковских кредитных карт, с их возможным последующим использованием для совершения незаконных финансовых операций (покупка товаров, либо отмывание денег) принято называть кардингом[2]. Повышенный интерес делинквентов к увеличению количества онлайн-платежей обуславливает необходимость совершенствования законодательства в области противодействия кардингу. Более того, низкий уровень противодействия в этой области превратил кардинг в самостоятельную сферу криминального бизнеса с огромной прибылью[3]. Анализ специальной и научной литературы позволяет нам сделать вывод о том, что противодействию хищениям денежных средств с банковских карт уделяется

---

[1] *Карпова Д.Н.* Киберпреступность: глобальная проблема и ее решение // Власть. М. 2014. № 8. С. 46.

[2] *Сачков Д.И., Смирнова И.Г.* Указ. соч. С 121.

[3] *Родивилин И.П.* Особенности характеристики состояния и структуры преступлений в сфере обращения охраняемой законом информации в современный период Российской Федерации // Вестник Восточно-Сибирского института МВД России. 2020. № 1. С. 66.

внимание со стороны научного сообщества. Однако, этой проблеме посвящено сравнительно мало работ[1]. В определенной мере она в юридической литературе исследовалась, однако в этих исследованиях не рассмотрены некоторые такие важные аспекты как уголовно-правовая квалификация, проблемы низкого темпа выявления и борьбы с этим явлением.

С развитием информационно-телекоммуникационной сети Интернет, информация еще больше внедряется в повседневную жизнь. Аудитория российского сегмента сети Интернет в 2017 году составила 87 миллионов человек[2], а в 2020 году этот показатель составлял уже 95,6 миллионов человек (78,1 % населения Российской Федерации в возрасте от 12 лет)[3]. Интерес в этом случае вызывает тот факт, что число пользователей сети Интернет в России, выходящих в киберпространство хотя бы раз за сутки, составляет 48% (56,3 млн. человек) населения. Согласно данным социологического опроса, проведенного Всероссийским центром изучения общественного мнения, 69 % россиян в возрасте от 18 лет и старше постоянно посещают сеть Интернет, 52 % россиян выходят в глобальную паутину ежедневно. Среди молодого поколения (18-24-летних) доля интернет-пользователей составляет 96 %[4]. Согласно результатам проведенного автором опроса студентов, 90 % респондентов ответили, что посещают глобальную сеть Интернет хотя бы раз в день, остальные 10 % – примерно раз в неделю. Таким образом, следует, что практически каждый

---

[1] См. *Акиндеева А.В.* Кардинг в сфере оборота банковских карт // Ученые записки Санкт-Петербургского им. В.Б. Бобкова филиала Российской таможенной академии. Спб., 2005. № 2 (24). С. 263-271; *Горбунов А.Н., Цимбал В.Н.* Способы незаконного использования пластиковых карт при совершении преступлений // Общество и право. № 3 (45). 2013. С. 217-221; *Октябрева М.С.* Кардинг в российской практике // Экономика и управление: анализ тенденций и перспектив развития. № 15. 2014. С. 99-103; *Павленко И.А., Смагоринский Б.П.* О современном состоянии расследования хищений денежных средств с использованием банковских карт на территории Российской Федерации // Вестник Волгоградской академии МВД России. 2012. № 1 (20). С. 166-172.

[2] Интернет в России: динамика проникновения. Лето 2017 г. // fom.ru Фонд Общественное Мнение. URL: http://fom.ru/SMI-i-internet/13783.

[3] Аудитория интернета в России в 2020 году // mediascope.net URL: https://mediascope.net/news/1250827.

[4] См.: Интернет: новая эра мобильных устройств // wciom.ru Всероссийский центр изучения общественного мнения (ВЦИОМ). URL: http://wciom.ru/index.php?id=236&uid= 115255.

гражданин РФ при несоблюдении правил безопасности при обращении с информацией ограниченного доступа подвергается риску виктимизации от преступлений в сфере обращения охраняемой законом информации.

Нормы об ответственности за преступления против охраняемой законом информации закреплены в гл. 28 УК РФ, а также присутствуют в некоторых статьях и рассредоточены по всей Особенной части УК РФ (ст. ст. 137, 138, 155, 183, 272, 273, 274, 274.1, 275, 276, 283, 283.1, 310, 311, 320).

Анализ статистических данных о количестве зарегистрированных преступлений по отдельным статьям не будет иметь научной и практической значимости. Представляется логичным рассмотреть данные ГИАЦ МВД России по форме 1-ИТТ «Сводный отчет о результатах деятельности ОВД РФ по противодействию преступлениям, совершенным с использованием информационно-телекоммуникационных технологий», который включает в себя сведения о преступлениях в сфере оборота охраняемой законом информации, совершенных с использованием:

1. средств мобильной связи;
2. вредоносных компьютерных программ;
3. информационно-телекоммуникационных технологий;
4. сети Интернет;
5. социальных сетей;
6. средств мгновенного обмена сообщениями (интернет-мессенджеров);
7. компьютерной техники;
8. расчетных (пластиковых) карт;
9. программных средств;
10. фиктивных электронных платежей;
11. электронных платежных систем;
12. криптовалют;
13. с использованием методов социальной инженерии;
14. с использованием SIP-телефонии.

Любой из этих способов направлен на получение доступа к охраняемой законом информации как самостоятельного преступления (ст. ст. 137, 138, 159.3, 159.6, 272, 273, 274, 274.1, п. «г» ч. 3 ст. 158 УК РФ и др.), так и в совокупности с другими статьями, на подготовку другого преступления (ст. ст. 105, 111, 158, 159 УК РФ и др.).

В 2020 года наблюдается резкий рост преступлений рассматриваемой категории – 510,4 тыс. преступлений, что на 73,4% больше, чем за 2019 год. В общем числе зарегистрированных преступлений их удельный вес увеличился и составляет – 25 %. Практически все такие преступления (98,6%) выявляются органами внутренних дел. Больше половины (58,8%) совершается с использованием сети «Интернет». Такой рост произошел за счет увеличения числа краж (ст. 158 УК РФ), совершаемых с использованием информации, а также мошенничеств (ст. 159 УК РФ). В 3 раза выросли нарушения неприкосновенности частной жизни (ст. 137 УК РФ) и нарушение тайны переписки, телефонных переговоров и иных сообщений (ст. 138 УК РФ).

График 1. Динамика уровня зарегистрированных преступлений по ст.137 (нарушение неприкосновенности частной жизни) и ст.138 (нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений) в Российской Федерации (2010-2020 гг.)

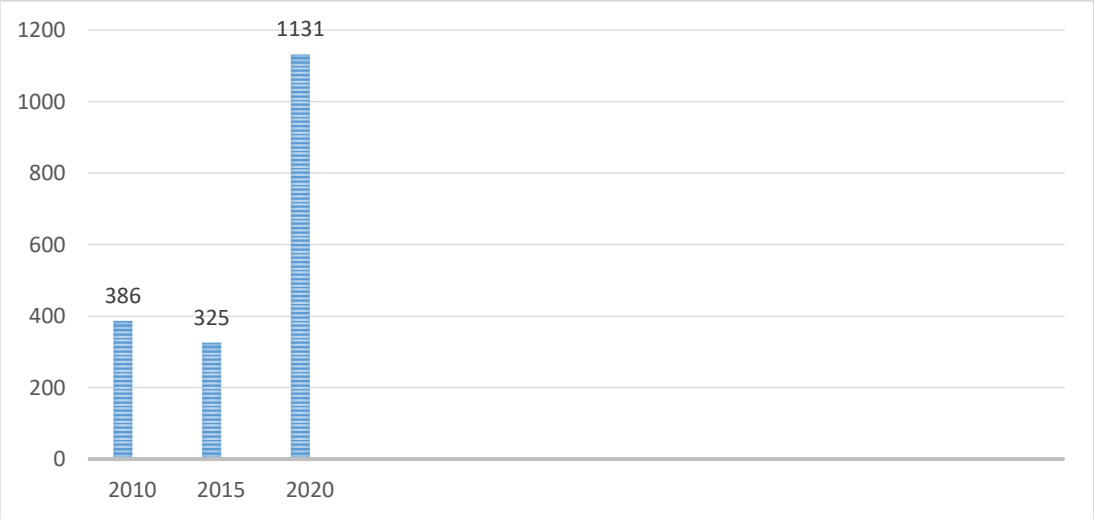
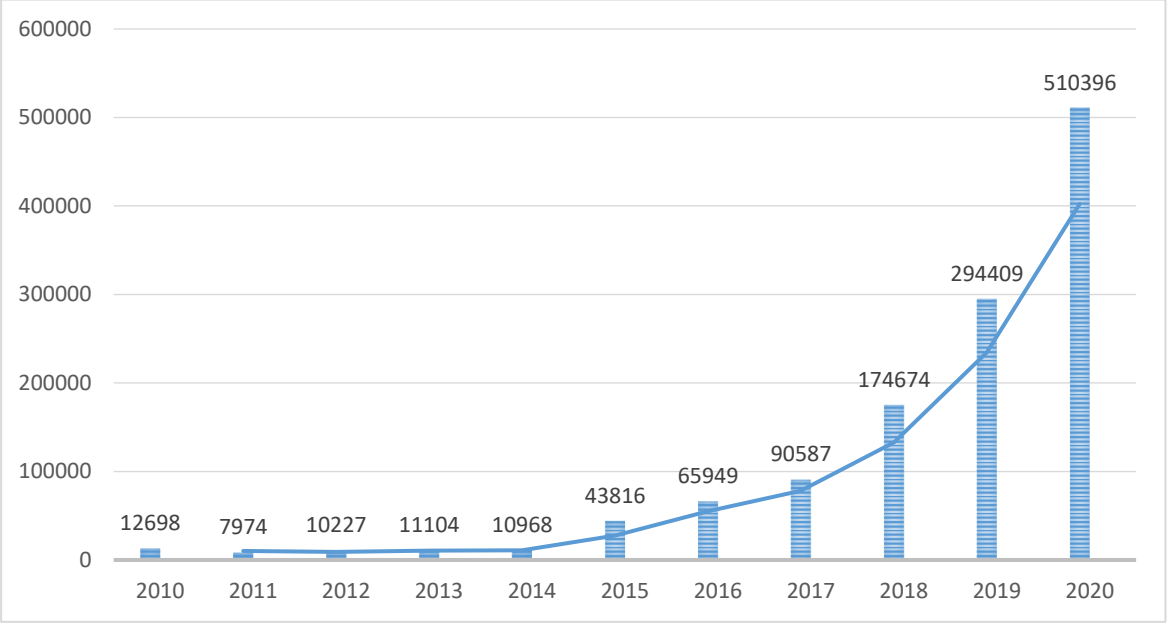


График 2. Динамика уровня зарегистрированных преступлений в сфере охраняемой законом информации в Российской Федерации (2010-2020 гг.)



Из приведенных данных видно, что динамика преступлений, совершенных в сфере охраняемой законом информации, характеризуется резким ростом с 2015 года. Такой рост произошел за счет увеличения числа краж (ст. 158 УК РФ), совершаемых с использованием информации с 2540 в 2014 г. до 9146 в 2015 г., а также мошенничества (ст. 159 УК РФ) с 2511 в 2014 г. до 14610 в 2015 г.

Таблица 1

Темпы прироста числа зарегистрированных преступлений в сфере обращения охраняемой законом информации за 2010-2020 гг.

Год	Количество преступлений	Абсолютный прирост	Темп прироста, %
2010	12698	-	-
2011	7974	-4724	-37,2
2012	10227	2253	28,3
2013	11104	887	8,6
2014	10968	-136	-1,2
2015	43816	32848	299,5
2016	65949	22133	50,5
2017	90587	24638	37,4
2018	174674	84087	92,8
2019	294409	119735	68,5
2020	510396	215987	73,4

Количество выявленных преступлений, нарушающих неприкосновенность частной жизни граждан, увеличивается в два раза на протяжении пяти лет. Это цена развития средств и возможностей информационного общества, когда глобальная информатизация всех сфер деятельности общества понижает степень его безопасности. Судебная практика отражает неблагоприятные тенденции роста посягательств на сохранность конфиденциальной информации о частной жизни лица[1].

Самую значительную долю в структуре преступлений в сфере обращения охраняемой законом информации, традиционно занимают преступления, связанные с неправомерным доступом к компьютерной информации – 57 % (см. табл. 2).

[1] *Хурум М.А*. Преступления, связанные с получением и (или) разглашением конфиденциальной информации: криминализация, систематизация и оптимизация законодательного описания: дис. … канд. юрид. наук. Краснодар., 2019. С. 59.

Таблица 2

Структура и динамика преступлений в сфере компьютерной информации, зарегистрированных в Российской Федерации за 2010-2020 гг. (%)

Статья УК РФ	Годы									
	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019
ст. 272 УК РФ	85,3	74,3	68,5	70,1	66,2	58,6	59,9	57,3	70	83,8
ст. 273 УК РФ	14,7	25,7	31,5	29,9	33,6	40,9	43	42,5	29,9	15,9
ст. 274 УК РФ	-	-	-	-	0,2	0,5	0,1	0,1	0,1	0,2
ст. 274^1 УК РФ	-	-	-	-	-	-	-	0,1	-	0,1

В 2019 году по сравнению с 2018 годом количество зарегистрированных преступлений в сфере компьютерной информации увеличилось на 383 или на 15.3%. Минимальный прирост зафиксирован в 2011 году (-4700 преступлений.). Темп наращения показывает, что тенденция ряда убывающая, что свидетельствует о снижении количества регистрируемых преступлений в указанной сфере до 2020 года. В 2020 году по сравнению с 2010 годом количество регистрируемых преступлений в сфере компьютерной информации уменьшилось на 2900 или на 39 % (см. табл. 2).

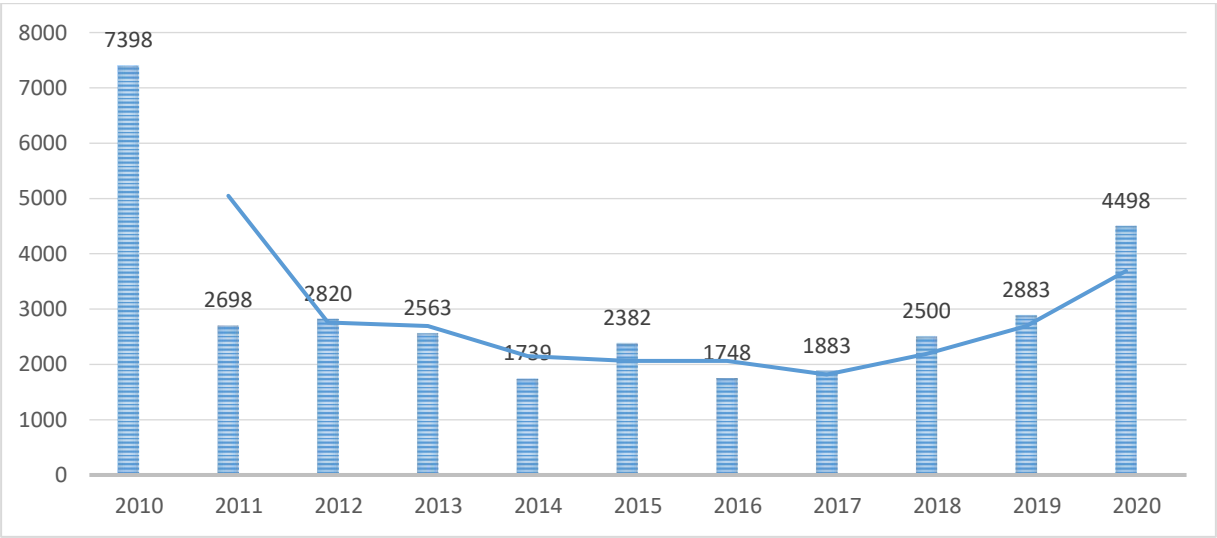
Таблица 3

Темпы прироста числа зарегистрированных преступлений в сфере компьютерной информации за 2010-2020 гг.

Год	Количество преступлений	Абсолютный прирост	Темп прироста, %	Темпы роста, %
2010	7398	-	-	100
2011	2698	-4700	-63.53	36.47
2012	2820	122	4.52	104.52
2013	2563	-257	-9.11	90.89
2014	1739	-824	-32.15	67.85
2015	2382	643	36.98	136.98
2016	1748	-634	-26.62	73.38
2017	1883	135	7.72	107.72
2018	2500	617	32.77	132.77
2019	2883	383	15.32	115.32
2020	4498	1615	56	156

Между тем количество исследуемых преступлений в общей структуре преступности невелико. Оно составляет сотые доли процентов.

График 3. Динамика уровня зарегистрированных преступлений в сфере компьютерной информации в Российской Федерации (2010-2020 гг.)



Преступления в сфере обращения охраняемой законом информации характеризуются большим количеством способов их совершения. Поэтому исследование структуры преступности в указанной сфере представляется крайне важным. Анализ изученных материалов уголовных дел по преступлениям, совершаемым в сфере оборота охраняемой законом информации, позволил нам выделить 6 основных способов.

Вполне естественно, что «лидером» среди исследуемой категории преступлений стало использование вредоносных компьютерных программ для мобильных телефонов – 53,0 %.

Достаточно близко к указанной категории примыкает неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам (16 %).

Достаточно большое количество обвинительных приговоров (10 %) вынесено по делам об использовании вредоносных компьютерных программ для неправомерного доступа к компьютерной технике (персональный компьютер, мобильный компьютер и т.п.).

По фактам скимминга обвинительные приговоры выносились в 9 % случаев.

Набирает популярность такой вид преступления как кардинг. Эта категория в общем количестве дел о преступлениях в сфере обращения охраняемой законом информации составила 8 %.

Еще 4 % дел возбуждалось по факту совершения ddos-атак.

График 4. Структура преступлений в сфере обращения охраняемой законом информации

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей выявлено лишь в 0,3 % случаев.

С трудовыми конфликтами связано 2 % дел. В этом случае сотрудник, недовольный своим увольнением или невыплатой обещанного вознаграждения, с целью отомстить руководству организации уничтожает, копирует или блокирует информацию. В ходе изучения уголовных дел установлено, что, что большинство преступлений (71,3 %) совершено в крупных городах, как правило, в столицах регионов Российской Федерации, 24,6 % – в городах с численностью населения более 50 тысяч человек, 4,1 % – в сельской местности. Около половины преступле-

ний в сфере обращения охраняемой законом информации совершено по месту жительства виновного (48,5 % дел). На рабочем месте преступником было совершено 24,6 % преступлений.

Большинство преступлений в сфере обращения охраняемой законом информации (89,5 %) являются длящимися либо совершаются неоднократно на протяжении значительного периода времени.

Развитие технологий стимулирует и преступников, совершающих преступления в сфере обращения охраняемой законом информации.

Снижение количества зарегистрированных преступлений в сфере компьютерной информации, на фоне огромного роста преступлений в сфере обращения охраняемой законом информации, что еще раз подчеркивает важность проведения данного исследования. Еще 10 лет назад криминологи указывали на высочайшие темпы роста преступлений в сфере компьютерной информации в России, что являлось основной тенденцией, характерной для преступлений в указанной сфере[1], однако, представление данные (см. таблицу 2) свидетельствуют о том, что количество регистрируемых преступлений в сфере обращения охраняемой законом информации с 2010 года постоянно снижается. Соотнося показатели 2016 и 2010 годов, можно заметить, что их число снизилось более чем в 4 раза, однако с 2016 года наблюдается устойчивая тенденция увеличения количества регистрируемых преступлений в сфере оборота охраняемой законом информации.

Снижение показателей по преступлениям в сфере обращения охраняемой законом информации, зафиксированное в статистических формах, связано со следующими обстоятельствами:

– правоохранительным органам стало сложнее выявлять преступления в сфере обращения охраняемой законом информации, ввиду появления новых способов их совершения (см. гл. 1), а также использования преступниками различных механизмов по сокрытию реальной личности в киберпространстве;

---

[1] *Лопатина Т.М.* Указ. соч. С. 10.

– пользователи информации стали более тщательно ее защищать, ограничивая доступ к ней сложными паролями. К выбору пароля пользователи стали относиться серьезнее, предпочтения отдаются достаточно длинным комбинациям, состоящим из больших и маленьких букв, цифр и символов.

Однако, можно обоснованно предположить, что современные статистические данные не в полной мере отражают реальное состояние преступности, в рассматриваемой сфере, в силу ее латентности.

Используя виктимологический опрос пострадавших от «информационных» преступлений лиц, а также экспертные оценки специалистов можно выяснить реальную криминогенную обстановку по преступлениям в сфере обращения охраняемой законом информации.

Согласно оценке экспертов[1] уровень латентности преступлений в сфере компьютерной информации следующим образом: от 0 до 25 % – 1,9 % опрошенных, от 26 до 50 % – 22,1 % респондентов, от 51 до 75 % – 28,8 %, от 76 до 90 % – 11,5 %, от 91 до 95 % – 15,0 %, от 96 до 99 % – 3,7 %, свыше 99 % – 4,0 %, затруднились ответить 13,0 % опрошенных. Из этого следует, что у респондентов складывается мнение, что в их поле зрения не попадает значительное количество преступлений в указанной сфере.

Попытаемся оценить уровень латентности умышленных преступлений в сфере обращения охраняемой законом информации на основе анализа иных источников.

Согласно сведениям, предоставленным АО «Инфовотч», российской компании, специализирующейся на информационной безопасности, следует, что количество инцидентов в сфере оборота охраняемой законом информации с каждым годом постоянно возрастает. В 2016 г. Аналитическим центром АО «Инфовотч» обнаружено 1556 случаев утечки конфиденциальной информации, что на 3,4 % превышает количество утечек в 2015 году. Число

[1] Оперуполномоченных подразделений «К» и следователей (102 человека)

неправомерного доступа к охраняемой законом информации в России в 2019 году выросло на 80 % по сравнению с 2016 годом[1].

Таблица 4

Динамика состояния неправомерного доступа к охраняемой законом информации и копирования информации в Российской Федерации (2010-2020 гг.)

Год	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Количество фактов неправомерного доступа к охраняемой законом информации	794	801	934	1143	1395	1505	1556	2456	2845	3598	4105

Также увеличивается количество скопированной информации, в результате неправомерного доступа, то есть качественный показатель.

Таблица 5

Динамика состояния количества случаев неправомерного доступа к охраняемой законом информации в Российской Федерации

Год	Объем персональных данных (млн.)	Абсолютный прирост	Темп прироста, %
2011	0,28	-	-
2012	0,40	0,12	42.86
2013	0,49	0,90	22.5
2014	0,55	0,06	12.24
2015	0,64	0,90	16.36
2016	2,02	1,38	215.63
2017	2,37	0,35	17.33
2018	2,87	0,50	21.1
2019	3,52	0,65	22.65

В 2019 г. по сравнению с 2018 г. количество утечек персональных данных увеличилось на 0,65 млн. единиц или на 22.7 %. Максимальный прирост

[1] INFOWATCH: Глобальное исследование утечек конфиденциальной информации // infowatch.ru. URL: https://www.infowatch.ru/report2019.

наблюдается в 2016 г. (1,38 млн. единиц.). Минимальный прирост зафиксирован в 2014 г. – 0,06 млн. единиц). Темп наращения показывает, что тенденция ряда возрастающая, что свидетельствует об увеличении объемов неправомерного доступа к персональным данным в Российской Федерации.

Проведенные автором опросы студентов показали, что менее 17 % респондентов уведомят правоохранительные органы в случаях нападений на информационные системы, а свыше 70% назвали в качестве основной причины отказа обращаться в правоохранительные органы – отсутствие уверенности в наказании виновных. Такое результат свидетельствует о высокой степени латентности преступлений в сфере обращения охраняемой законом информации.

Сходные тенденции характерны не только для нашей страны. Согласно экспертным данным, в мире ежегодно наблюдается рост компьютерной преступности и производного от них размера ущерба[1].

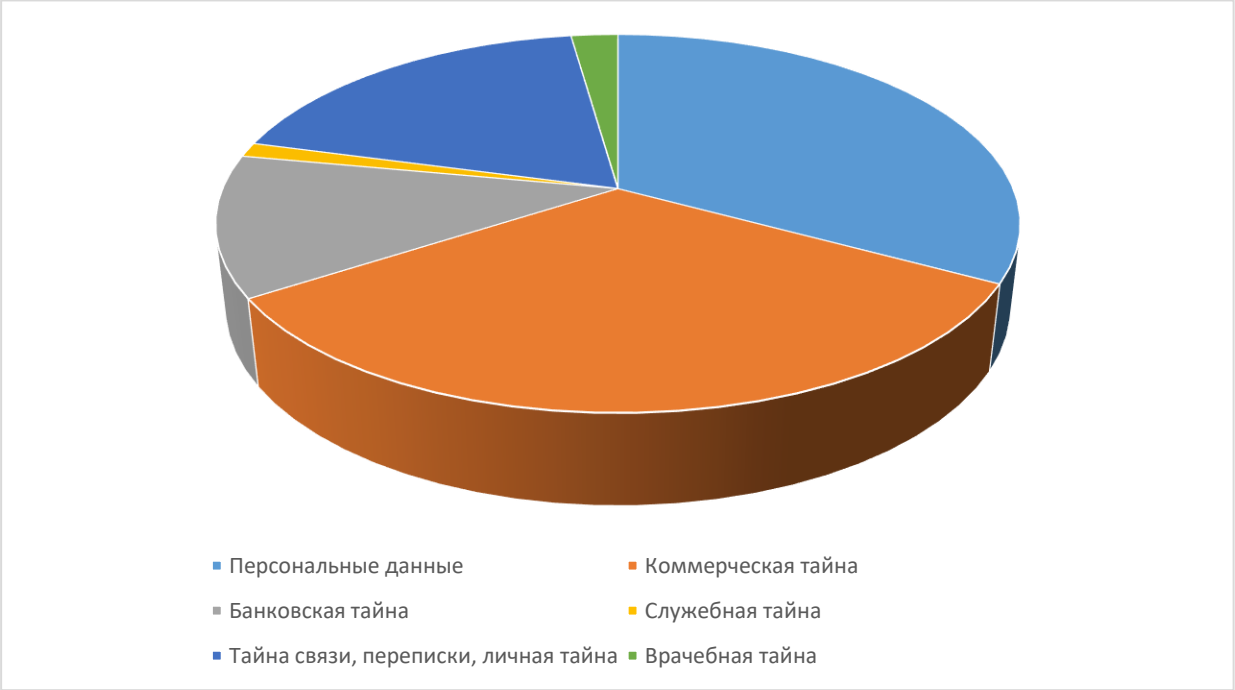
Появление новых способов совершения преступлений в сфере обращения охраняемой законом информации. Процесс совершенствования способов совершения преступлений в сфере обращения охраняемой законом информации постоянно развивается. Необходимо указать на новый вид преступлений в сфере обращения охраняемой законом информации, связанный с электронными платежами через сеть Интернет. Через глобальную паутину можно оплатить мобильную связь, услуги ЖКХ, штрафы, купить товар в интернет-магазине и т.д. На сегодняшний день наиболее распространённым средством платежа является пластиковая банковская карта, однако виртуальные финансовые операции не ограничиваются только использованием пластиковых платежных карт. Все чаще стали использоваться сервисы электронных платежей, такие как «Яндекс.Деньги», «WebMoney», «Qiwi», «Paypal» и др.

---

[1] См. более подробнее: Лацинская М. Group-IB представила отчет о хакерских атаках // Газета.Ру. 2016 г. 13 окт. URL: https://www.gazeta.ru/tech/2016/10/13/10249697/cybercrimecon_2016.shtml.

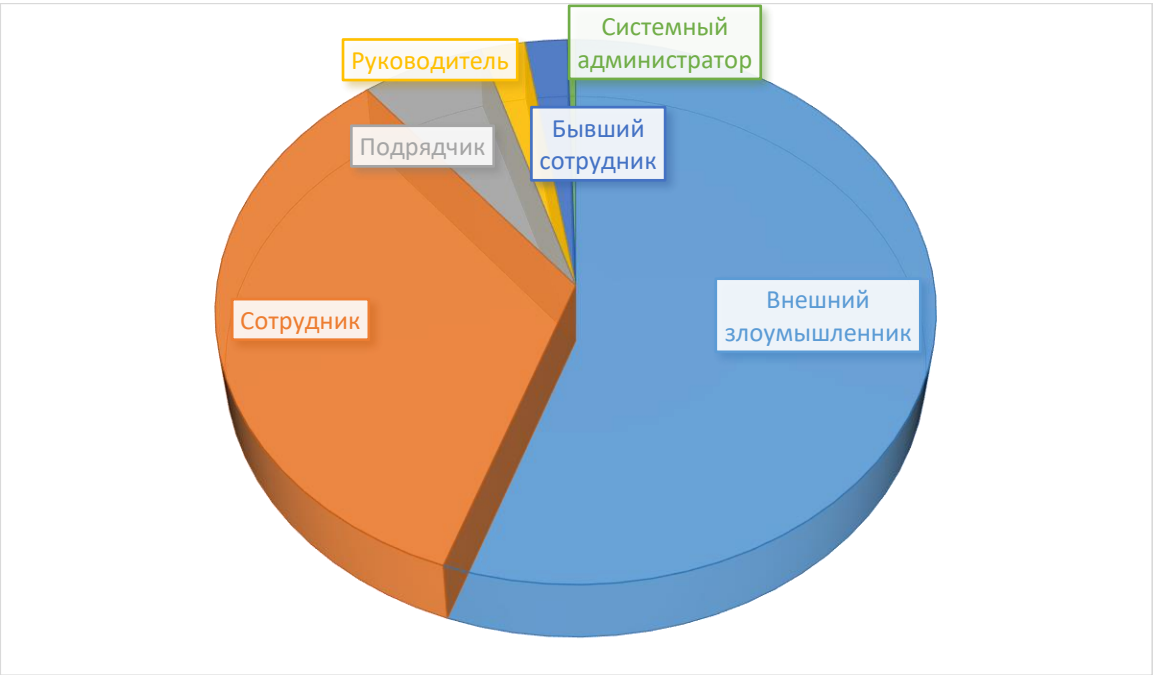
В большинстве случаев предметом преступного посягательства становится охраняемая законом информация, содержащая сведения о персональных данных граждан, коммерческая тайна.

График 5. Структура охраняемой законом информации, подвергаемой неправомерному доступу в Российской Федерации в 2020 г. (доля в %)



Неправомерный доступ к охраняемой законом информации совершается по вине лиц, являющихся работниками организаций, пострадавших от действий злоумышленников (61,8 %), однако действия по неправомерному доступу совершает лицо, не являющееся работником организации.

График 6. Структура неправомерного доступа к охраняемой законом информации в Российской Федерации за 2015-2020 гг.



Совершение преступлений в сфере обращения охраняемой законом информации, направленных на получение информации, находящейся в мобильных устройствах, связано с увеличением в России количества мобильных телефонов и другой носимой электроники. Пользователи фотографируют бумажные документы, экран рабочего монитора, отправляют фотографии и файлы с помощью мессенджеров и облачных сервисов.

Подводя итоги анализа состояния преступности в сфере обращения охраняемой законом информации можно сделать следующие выводы:

1. Как следует из проведенного анализа, количество регистрируемых преступлений в сфере обращения охраняемой законом информации увеличивается. 25 % всех зарегистрированных преступлений совершаются либо с незаконным использованием охраняемой законом информации, либо она сама становиться предметом преступления. Однако наблюдается снижение преступлений в сфере компьютерной информации, что обусловлено, с одной

стороны, появлением новых схем противоправных деяний, с другой, изменением отношения пользователей к своей информации ограниченного доступа.

2. Количество зарегистрированных преступлений в указанной сфере с 2015 года постоянно растет.

3. Преступления указанной категории обладают высоким уровнем латентности, для них характерно появление новых способов совершения преступлений.

4. Установлено, что предметом преступного посягательства в большинстве случаев становятся персональные данные.

5. Неправомерный доступ к охраняемой законном информации, в большинстве случаев, совершается по вине лиц, являющихся работниками организаций, пострадавших от действий злоумышленников.

§ 2. Личность преступника, совершающего преступления в сфере обращения охраняемой законом информации

В общем анализе личности преступника, совершающего преступления в сфере оборота охраняемой законом информации, с нашей точки зрения, необходимо рассмотреть классификацию преступников, дать им криминологическую характеристику.

Другим важным обстоятельством, которое следует учитывать при изучении личности преступника, совершающего преступления в сфере обращения охраняемой законом информации – стирание государственных границ. Другими словами, преступления в отношении российских граждан совершаются не только гражданами РФ, но и иностранными гражданами. В научной литературе мало внимания уделяется этому факту.

Лицо, совершившее преступление в сфере обращения охраняемой законом информации, заранее предусматривает возможности его выявления и в связи с

этим подыскивают наиболее эффективные приемы по противодействию этому, применяя логические приемы.

Современные преступники, специализирующиеся на преступлениях в сфере обращения охраняемой законом информации, не являются одиночками, а собираются в группы, члены которой зачастую находятся в разных регионах нашей страны или за ее пределами. Однако в цифрах официальной статистики этот факт не нашёл своего отражения. По нашему мнению, это объясняется, во-первых, сложностью выявления преступных связей субъекта преступления, во-вторых, сложностью доказывания формы соучастия в преступлении, что также обусловлено использованием мессенджеров с шифрованием электронных сообщений, общение на форумах в сети TOP[1], использованием криптовалют для распределения дохода, полученного преступным путем.

Указанные средства коммуникации между участниками преступной группы, в силу их анонимности, не позволяют доказать преступный сговор между ними. Преступные формирования хакеров практически закрыты для посторонних, и очень трудно проводить в отношении них оперативно-розыскные мероприятия в силу специфики их преступной деятельности и удаленности от объекта преступного посягательства[2].

На просторах Интернета имеется обилие ресурсов, объединенных едиными убеждениями – совершать преступления в киберпространстве. Следует обратить внимание на то обстоятельство, что участники преступной группы в большинстве случаев никогда не встречались друг с другом лицом к лицу и проживают в разных регионах мира. Все общение между ними происходит с использованием информационных средств коммуникации через сеть Интернет, практически всегда с использованием программного обеспечения, позволяющего анонимно общаться

---

[1] Свободное и открытое программное обеспечение для реализации второго поколения так называемой луковой маршрутизации. Это система прокси-серверов, позволяющая устанавливать анонимное сетевое соединение, защищённое от прослушивания. Рассматривается как анонимная сеть виртуальных туннелей, предоставляющая передачу данных в зашифрованном виде.

[2] *Морар И.О.* Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления // Российский следователь. 2012. №13. С. 34–37.

в киберпространстве. Информационные воры – это не Робин Гуды, они работают из корыстной заинтересованности, однако иногда встречаются лица, совершающие преступления с целью проверить свои навыки.

Круг лиц, совершающих преступления в сфере обращения охраняемой законом информации, не ограничивается только «хакерами». К лицам, совершающим преступления в сфере обращения охраняемой законом информации, следует применять термин «информационные воры», так как их целью является похищение важного в современном мире ресурса – информации. Информационные воры являются частью отдельной категории преступников, которых принято называть киберпреступниками.

Проведенное автором исследование личности, осужденных за преступления рассматриваемой категории, позволяют сделать вывод о том, что большинство преступников были в возрасте от 19 до 40 лет (74 %). Средний возраст преступников – 26 лет, при этом 56,1 % приходится на группу в диапазоне от 19 до 24 лет.

Таблица 6

Структура возрастных групп лиц, совершивших преступления в сфере обращения охраняемой законом информации.

Возраст	Доля среди общего числа в %
До 19 лет	18,8 %,
20-24 года	37,3 %,
25-29 лет	17,9 %,
30-34 года	11,3 %,
35-39 лет	7,1 %
40 лет и старше	7,6 %

Доля женщин составляет 1 %. При оценке образовательного уровня следует учитывать, что 21,7 % – это студенты высших (18,9 %) и средних (2,8 %) профессиональных учебных заведений. Установлено, что 30,7 % преступников

имеют высшие образование, 16,5 % – неполное высшее, 16,5 % – средне профессиональное, 34,0 % – среднее, остальные 2,3 % – с неполным средним образованием.

По роду занятий изученные преступники распределились следующим образом: 21,7 % – это учащиеся и студенты (все – мужчины), 9,4 % – программисты (все – мужчины), 6,1 % – инженеры (техники) по обслуживанию и ремонту компьютерного оборудования (все – мужчины), 2,8 % – бухгалтеры и другие специалисты в кредитно-финансовой сфере (мужчин и женщин – по 50 %), 15,1 % – руководители различных уровней в коммерческих организациях (мужчин – 96,9 %, женщин – 3,1 %), 9,9 % – частные предприниматели (мужчин – 95,2 %, женщин – 4,8 %), 7,6 % – продавцы и торговые представители (мужчин – 75 %, женщин – 25 %), 1,9 % – государственные служащие (все – мужчины), 9,0 % – работники иных профессий (мужчин – 73,7 %, женщин – 26,3 %), 16,5 % – временно не работающие (мужчин – 85,7 %, женщин – 14,3 %).

Всего же среди совершивших преступления 54,2 % лиц, работа (обучение) которых так или иначе связана с компьютерными технологиями, из них 56,0 % от числа мужчин и 36,8 % от числа женщин. Имели достаточные познания в данной области 82,1 % осужденных – 86,5 % мужчин и 36,8 % женщин.

Практически все изученные осужденные – граждане Российской Федерации. Лишь 3 % преступников были гражданами Молдавии.

Большинство преступников проживали в крупных городах, как правило, в столицах регионов Российской Федерации – 73,1 %. В городах с численностью населения более 50 тысяч человек проживало 24,6 % лиц. Еще 4,1 % осужденных проживало в сельской местности.

Обычно преступления в сфере обращения охраняемой законом информации совершаются в одиночку (85,6 %), в соучастии совершено 14,4% преступлений. В одиночку совершались преступления, источником которых послужили конфликты с работодателями (100 %). Подавляющее большинство преступников (87 %) знали об ответственности за совершение преступлений в указанной сфере, однако

частная превенция здесь не сработала. У этих людей не были сформированы позитивные убеждения, взгляды и нормы морали.

Причинами этому служит: мягкость наказания за совершение преступления в сфере обращения охраняемой законом информации; недоквалификация преступного деяния, например, признание неправомерного доступа к охраняемой законом информации способом совершения кражи и т.п.

13% преступников пояснили, что не догадывались о том, что совершают преступления в сфере обращения охраняемой законом информации. Это касается категорий преступлений, совершенных в совокупности с иными статьями особенной части УК РФ (183, 158, 159, 159[6]), где доступ к охраняемой законом информации не охватывался прямым или косвенным умыслом и являлся подготовкой к совершению преступления.

В научной литературе встречается мнение о том, что, изучая способ совершения преступления в сфере компьютерной информации, можно дополнить личностную картину преступника[1].

Следует согласиться с Ю.А. Мерзловым, утверждающим, что представление характерологических особенностей личности преступника, совершающего противоправные посягательства в сфере обращения охраняемой законом информации, целесообразно осуществить через типологию соответствующих лиц, применительно к тому или иному виду преступного деяния[2].

Автором было проведено самостоятельное криминологическое исследование, в результате которого были интерпретированы эмпирические данные, полученные в ходе проведения анкетирования оперативных сотрудников, следователей, сотрудников прокуратуры, изучения материалов уголовных дел (материалы доследственных проверок, постановления об отказе в возбуждении уголовного дела, обвинительные заключения, обвинительные приговоры и другие

---

[1] *Морар И.О.* Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия? // Российский следователь. 2012. № 12. С. 37–41.

[2] *Мерзлов Ю.А.* Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. 2015. № 4 (7). С. 57.

процессуальные документы)[1]. На основе полученных данных составлены актуальные схемы совершения преступлений рассматриваемой категории, используемые злоумышленниками за последнее время, и на их основе сделана типология лиц, совершающих эти противоправные деяния.

Способы совершения преступления были положены в основу классификации личности преступника, совершающего преступления в сфере обращения охраняемой законом информации. Исходя из предложенной классификации, предлагаем разделить лиц, совершающих преступления в указанной сфере на следующие виды.

1. Лица, использующие вредоносные компьютерные программы для мобильных телефонов. Подобную схему хищения денежных средств сложно организовать одному человеку. Как правило, функции распределены между несколькими участниками преступной группы. В работах специалистов в области информационной безопасности давно устоялось мнение о том, что «современный киберпреступник уже не пират-одиночка, а звено в серьезном криминальном бизнес-процессе. Каждый из них выполняет свою роль в процессе производства и реализации вредоносного программного обеспечения»[2]. Указанную категорию лиц следует разделять на следующие виды:

– Непосредственно вирусописатель – это лицо, написавшее вредоносный программный код. Вирусописатель обладает специальными познаниями в сфере информационных технологий, имеет высшее образование, редко является самоучкой. Обычно, это мужчина, возраст от 25 до 40 лет, женатый, имеющий высшее образование, городской житель с постоянной трудовой занятостью в области информационной безопасности (системный администратор, программист и т.п.), как правило, ранее несудимый, но до попадания в поле зрения правоохранительных органов, совершающий подобные

---

[1] *Родивилин И.П.* Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. 2017. № 4 (67). С. 25-29.

[2] *Унучек Р.С.,* Мобильные угрозы // Вопросы кибербезопасности. 2014. № 3(4). С. 57.

преступления неоднократно. По характеру является целеустремленным, изобретательным человеком. Использует свои знания и навыки для достижения преступной цели. Хорошо знаком с нормами, устанавливающими уголовную ответственность за совершение преступлений в сфере обращения охраняемой законом информации, и относится к ним в целом положительно, однако надеется, что не будет разоблачен благодаря своему профессионализму.

– «Заливщик» – человек, который предпринимает действия для того, чтобы жертва установила вредоносную программу на свое мобильное устройство. Как правило, это рассылка спама или ссылок на объявление на популярных сайтах. В большинстве случаев это мужчина, возраст от 18 до 30 лет, имеющий средне-специальное или неоконченное высшее образование, городской житель с непостоянным источником заработка или нигде неработающий, не женат, ранее несудимый. По характеру является оригинальной, нестандартной личностью, обладающей интеллектом выше среднего, позволяющим ему находить нестандартные способы «залива» вредоносной компьютерной программы на устройство жертвы. К своим преступным действиям относится как к источнику заработка и не считает себя преступником, к закону относится с неуважением, часто совершает административные правонарушения.

– Лица, администрирующие интернет-ресурс, на котором отображаются данные о «зараженных» устройствах (администраторы). Данная категория лиц, обладает познаниями в сфере компьютерных технологий и, как правило, является самоучками, так как углубленных познаний в области программирования не требуется. Как правило, это мужчина, возраст от 20 до 35 лет, неженатый, нигде не работающий, без образования или имеющий средне-специальное образование, ранее несудимый либо судимый за нетяжкие общеуголовные преступления. По характеру является спокойным, уравновешенным, внимательным человеком, что помогает ему администрировать (управлять) вредоносными сайтами в сети Интернет.

– «Дроп» – это лицо, осуществляющее обналичивание денежных средств. Обычно это молодой человек, возраст от 20 до 40 лет, неженатый, студент либо нигде не работающий, имеющий среднее или средне специальное образование, нередко лицо без определенного места жительства, ранее судимый за преступления, не связанные с компьютерной информацией. «Дроп» является самой низшей кастой в иерархии рассматриваемых преступников. Как правило самый уязвимый участник преступной группы, в силу того, что является последним звеном в хищении денежных средств и в отличии от остальных участников преступной группы, совершает свои действия не в виртуальном пространстве. Понимая последствия своих действий, тяжесть совершаемого преступления и высокий риск быть пойманным, «дроп» также является самой опасной категорией преступников, совершающих преступления в сфере обращения охраняемой законом информации. Как правило, при задержании сотрудниками правоохранительных органов он оказывают сопротивление, нередко вооружен. Заранее продумываются варианты противодействия правосудию, как правило, свою вину не признает. По характеру является агрессивным, злобным человеком. К закону относится с пренебрежением. Совершает преступления из корыстной заинтересованности, а вид источника преступного дохода не имеет значения (не является принципиальным выбор между совершением компьютерного преступления или общеуголовного).

– Организатор – лицо, организовавшее преступную схему, связующее звено между заливщиками, «администраторами», дропами и вирусописателем (иногда сам является автором вируса). Организатор, как правило, это мужчина, возраст от 25 до 40 лет, женатый, имеет высшее или средне-специальное образование, имеет постоянную трудовую занятость в области информационной безопасности (системный администратор, программист и т.п.), ранее несудимый или судимый за преступления экономической направленности. В нравственно-мотивационной сфере у указанной категории лиц наблюдалось стремление быстро разбогатеть, приложив минимум усилий, используя лишь свои познания в

сфере информационных технологий. В системе их ценностей лидирующие позиции отводятся индивидуальным ориентациям.

В ходе опроса сотрудников предварительного следствия Восточно-Сибирского региона, которые осуществляют расследование рассматриваемой категории уголовных дел, установлено, что доля нераскрытых преступлений составляет 96 %. Опрошенные респонденты в качестве основной причины такой ситуации указали на то обстоятельство, что злоумышленники находятся в других субъектах Российской Федерации или заграницей, в связи с чем их поиск и привлечение к уголовной ответственности представляется затруднительными. В случае установления факта совершения преступления преступной группой, далеко не всегда удается выявить всех ее участников.

2. Лица, использующие вредоносные компьютерные программы для неправомерного доступа к компьютерам, ноутбукам и т.д. В отличие от рассмотренной выше группы преступлений, подобного рода деяния могут совершаться как преступниками-одиночками, обладающими необходимыми знаниями в программировании, так и группой лиц. Ряд авторов при криминологической характеристике личности преступников, занимающихся незаконным оборотом вредоносных компьютерных программ, в зависимости от характера совершаемых деяний и различий в профессиональных навыках разделяют этих лиц на три группы: создателей, пользователей и распространителей[1]. Хотя и существует такое разделение, но преступники действуют поодиночке, не собираясь в преступные группы и не действуя сообща. Каждый выполняет определённую роль за вознаграждение. По преступной схеме подобного рода действуют мужчины, имеющие высшее или средне-специальное образование, возраст от 18 до 40 лет, неженатые, ранее несудимые, городские жители или переехавшие в город из сельской местности, студенты или служащие, как правило, интеллектуальное развитие у них на высоком уровне. Говоря о

---

[1] *Маслакова Е.А.* Указ. соч. С.9.

нравственно-психологической характеристике лиц указанной категории, необходимо обратить внимание на то обстоятельство, что этот тип преступника, совершая преступления, удовлетворяет сразу две свои потребности: самоутвердиться и улучшить свое материальное благосостояние, используя свои знания.

3. Лица, осуществляющие неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам. Совершается преступниками-одиночками, не имеющими образования в информационной сфере. В большинстве случаев преступления совершаются из корыстной заинтересованности, в редких случаях, с целью проверить свои навыки. Нет четкого разграничения по возрасту, образованию и социальному статусу. Таким преступником может являться как школьник, студент, так и кандидат наук. Обычно это мужчина, в возрасте от 16 до 40, неженатый. Как правило, злоумышленники понимают, что они совершают противоправные действия, но надеются избежать наказания, используя свои познания в сфере информационных технологий. По отношению к жертве испытывают презрение, иногда осуждают ее за виктимное поведение (использование простого пароля для ограничения доступа к учетной записи в социальной сети или электронному почтовому ящику; использование одного пароля ко всем учетным записям в социальных сетях, что облегчает неправомерный доступ). Предпочитают переписку через Интернет любой другой форме общения (так называемые «текстроверты»), так как являются застенчивыми, стеснительными людьми. В виртуальном пространстве на различных форумах им проще выразить свои чувства и эмоции.

В отдельную подкатегорию можно выделить лиц, совершающих хищение «цифровой личности». В сети Интернет в настоящий момент можно купить не только живого человека, но и «цифровую личность»[1]. Кража данных – это серьезная угроза для всех пользователей, ее последствия проявляются как на

[1] *Жмуров Д.В.* Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1. С. 90.

индивидуальном, так и на общественном уровне. Стоимость может варьироваться от 1 до 100 долларов США в зависимости от личности[1]. Используются ворованные «цифровые личности» разными типами злоумышленников, например, лицами, которые размещают рекламу в интернете и переправляет трафик (пользователей) на товар рекламодателя, зарабатывая комиссию с каждой продажи – «арбитражники трафика». В целом их деятельность в киберпространстве является легальной (за исключением лиц, размещающий рекламу на адалт-трафик – порно-сайты, эротические онлайн-трансляции и т.п., которые подпадают под уголовное преследование по ст. 133, 135, 242, 242.1, 242.2 УК РФ). Для продвижения рекламы «арбитражнику» нужно иметь много учетных записей в социальных сетях, чтобы с их помощью заниматься рассылкой сообщений, добавлением в список друзей, написания комментариев в тематических сообществах. Для них важную роль имеет тот факт, чтобы учетная запись в социальной сети была правдоподобной. Для этой цели они использует специальные сайты в сети Интернет, на которых продаются реквизиты доступа к аккаунтам реальных людей. Тем самым они совершают неправомерный доступ к информации, размещенной в учетной записи и нарушают тайну переписки. Выявлять таких лиц сложно. Мошенники тоже используют цифровые личности, для обмана лиц, которые присутствуют в списке друзей украденного аккаунта[2].

4. *Кардеры* – лица похищающие реквизиты, идентифицирующие пользователей в сети Интернет как владельцев банковских кредитных карт, с их возможным последующим использованием для совершения незаконных финансовых операций (покупка товаров либо отмывание денег)[3]. Последнее время появился вид виртуальных кардеров – Вэб-кардеры, то есть лица, осуществляющие хищения денежных средств со счетов платежных карт,

---

[1] «Цифровая личность» за копейки // www.comnews.ru URL: https://www.comnews.ru/content/115730/2018-11-12/cifrovaya-lichnost-za-kopeyki.

[2] Архив Кировского районного суда г. Иркутска, 2017 г., уголовное дело № 1-182/17; Архив Кировского районного суда г. Иркутска, 2018 г., уголовное дело № 1-264/2018; Архив Кировского районного суда г. Иркутска, 2020 г., уголовное дело № 1-53/2020.

[3] *Сачков Д.И., Смирнова И.Г.* Указ. соч. С. 29.

виртуальных счетов, криптовалюты с использованием сети Интернет. Лиц, занимающихся хищением денежных средств по подобной схеме, именуют «кардером» или «Вэб-кардером». Кардингом занимаются нигде не работающие мужчины, так как подобного рода деятельность отнимает практически все время. Возраст злоумышленников от 18 до 40 лет, не женаты. Как правило, это люди без образования или имеющие неоконченное высшее образование, ранее не судимы. Являются очень работоспособными людьми. Для совершения хищений, например, с американских платежных карт, переходят на режим бодрствования и сна, схожий с часовым поясом США.

5. Лица, совершающие хищение денежных средств, используя «Скиммер». Эти лица имеют разный социальный статус, возраст от 18 до 50 лет, нигде не работающие или студенты, процент женатых и холостых примерно на одном уровне, ранее несудимые или судимые за общеуголовные преступления. Обычно этими преступлениями занимаются организованные группы, так как одному человеку сложно выполнить все действия, необходимые для совершения хищения денежных средств: прикрепить «Скимминг», следить за ним (чтобы его не обнаружили), через несколько часов снять, расшифровать записанные данные и записать на фальш-карты. По характеру являются бесстрашными, хладнокровными людьми, что позволяет им не обращать внимание на страх быть пойманным в момент постановки или снятия скиммингового оборудования.

6. Лица, осуществляющие Ddos-атаки. Такие преступления совершаются в одиночку. Как правило, это мужчина, возраст от 20 до 40 лет, не женат, неработающий, без высшего образования и без специального образования в области информационных технологий, ранее не судим. По характеру является замкнутым и зажатым человеком, предпочитающим виртуальное общение реальному.

Подводя итог проведенного криминологического анализа лиц, совершающих преступления в сфере обращения охраняемой законом информации, сформулируем основные выводы:

1. Изучение особенностей лиц, совершающих преступления, является важным условием правильной организации борьбы с определенным видом преступной деятельности. Для преступлений в сфере обращения охраняемой законом информации, изучение личности преступника приобретает особую актуальность, так как в данном случае речь идет о субъектах, которые до недавнего времени не попадали в поле зрения правоохранительных органов.

2. Анализ уголовных дел показывает, что подобные преступления в подавляющем большинстве совершаются лицами мужского пола, среди которых преобладают молодые люди в возрасте от 19 до 24 лет (56,1 %).

3. Круг лиц, совершающих преступления в сфере обращения охраняемой законом информации, не ограничивается только «хакерами». К лицам, совершающим преступления в сфере обращения охраняемой законом информации, следует применять термин «информационные воры», так как их целью является похищение важного в современном мире ресурса – информации. Информационные воры являются частью отдельной категории преступников, которых принято называть киберпреступниками.

4. Изучение личности информационных воров с точки зрения способов совершения противоправных деяний, обладающих схожими чертами, несомненно может способствовать раскрытию и профилактике преступлений в сфере обращения охраняемой законом информации.

§ 3. Факторы, детерминирующие совершение преступлений в сфере обращения охраняемой законом информации

Анализ криминальной ситуации, сложившейся в сфере оборота охраняемой законом информации, свидетельствует о том, что посягательства на информацию носят массовый характер. Объем похищаемых данных настолько велик[1], что еще раз подтверждает необходимость самого серьезного внимания со стороны

[1] См. параграф 1.

государства к этой проблеме и принятия решений по предупреждению преступлений в сфере оборот охраняемой законом информации. Совершать преступления такого рода с одной стороны выгодно[1], с другой достаточно безопасно для преступника (раскрываемость подобного рода преступлений составляет 18 %)[2].

Общими детерминантами для всех преступлений являются: экономический кризис, рост цены товаров, снижение уровня жизни, повышение уровня безработицы и т.д. Детерминанты преступлений в сфере оборота охраняемой законом информации, на наш взгляд, обусловлены, в первую очередь, особенностями киберпространства и информационно-телекоммуникационных технологий. Использование возможностей киберпространства облегчает процесс совершения преступления на каждом этапе, позволяет оставаться анонимным и не привлекать к себе лишнее внимание со стороны правоохранительных органов, снижает риск быть пойманным. Поэтому в связи с тематикой исследования особое внимание, на наш взгляд, следует уделить специальным детерминантам преступлений в сфере оборота охраняемой законом информации.

Любая преступность, как правило ситуативная, то есть для того чтобы преступление произошло необходимо чтобы совпало три фактора – мотивированный преступник, подходящая жертва, отсутствие внешнего контроля[3]. Из этих трех условий можно выделить следующие факторы, влияющие на совершения преступлений в сфере охраняемой законом информацию.

В ходе проведенного автором исследования[4] выявлены криминогенные факторы совершения преступлений в сфере обращения охраняемой законом информации, которые можно разделить по следующим основаниям.

---

[1] Киберпреступность в цифрах // www.aktiv-company.ru URL: https://www.aktiv-company.ru/analitics/articles/cybercryme.html.

[2] Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года // www.mvd.ru URL: https://xn--b1aew.xn--p1ai/reports/item/22678184.

[3] *Shah S.A.* Biological and Psychophysiological Factors in Criminality / S.A. Shah, H.R. Loren. Handbook of Criminology. Chicago: Rand McNally, 1974.-Pp. 101-173.

[4] *Родивилин И.П.* Современная специфика детерминации преступлений в сфере обращения охраняемой законом информации // Вестник УДГУ. 2021. № 2. С. 305-311.

Факторы правового характера. Одной из причин компьютерной преступности является анемия, слабость норм. Е.П. Ищенко одним из условий, способствующих криминализации киберпространства, а значит и влияния на рост преступлений в сфере обращения охраняемой законом информации, считает отставание законодательного регулирования от возможностей противоправного использования информационно-коммуникационных технологий, темпов информатизации всех сфер общественной жизни[1]. Отсутствие единого понятийного аппарата, регламентирующего преступления в сфере оборота охраняемой законом информации, информатизация всех сфер общественной жизни, отсутствие уголовной ответственности за ограничение доступа к охраняемой законом информации и другие проблемы уголовно-правового характера[2], также влияют на развитие и рост преступлений в сфере обращения охраняемой законом информации.

Ввиду высокой степени анонимности сети Интернет и низкого уровня правового регулирования, можно заключить, что сеть Интернет становится преступной средой, в которой процесс поиска как правонарушителей, так и жертв преступлений становиться весьма затруднителен.

В Российской Федерации на сегодняшний день существует механизм, благодаря которому государство получило возможность осуществлять регулирование в сети Интернет. Так, согласно ФЗ № 149-ФЗ существует 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. К такой информации относятся: материалы с порнографическими изображениями несовершеннолетних; информация о способах, методах разработки, изготовления и использования наркотических средств; информация о способах совершения самоубийства, а также призывов к совершению самоубийства; информация о несовершеннолетнем, пострадавшем в результате противоправных действий

---

[1] *Ищенко Е.П.* Киберпреступность: криминалистический аспект проблемы // Библиотека криминалиста. 2013. № 5. С. 189

[2] Рассмотренные в 1 главе настоящего исследования.

(бездействия); информация, нарушающая требования Федерального закона от 29 декабря 2006 года № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 года № 138-ФЗ «О лотереях», о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети Интернет и иных средств связи. Однако такое регулирование со стороны государства является малоэффективным в силу отсутствие механизмов контроля за сетью Интернет, которое обусловлено ее транснациональностью[1].

Технические факторы. Рост количества компьютерной техники, используемой в России, приводит и к росту числа пользователей охраняемой законом информации, а также к увеличению ее объемов. Этому способствует снижение цен на компьютеры и периферийное оборудование (принтеры, сканеры, модемы и др.). К техническим факторам, детерминирующим преступления в сфере обращения охраняемой законом информации, также можно отнести недостаточность защиты самих технических средств защиты компьютерной техники.

Как показывает проведенный анализ, несовершенство системы защиты от несанкционированного доступа к компьютерной технике и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя, также является криминогенным фактором, способствующим совершению преступлений в сфере обращения охраняемой законом информации. Самыми распространенными ошибками пользователей информации, приводящими к неправомерному доступу и копирования информации, являются:

1. потеря съемных носителей;
2. потеря мобильных устройств (в т.ч. в результате кражи);
3. небрежное обращение с бумажными документами;

---

[1] *Номоконов В.А., Тропина Т.Л.* Киберпреступность: прогнозы и проблемы борьбы // Библиотека криминалиста. 2013. № 5 (10). С. 148 -160.

4. ошибочное предоставление прав доступа, выкладывание закрытой информации в общий доступ;

5. передача оборудования, содержащего информацию ограниченного доступа, на техническое обслуживание третьим лицам;

6. нарушение политики безопасности (нелегитимная пересылка, копирование информации) по просьбе других сотрудников и прочих лиц (социальная инженерия);

7. нарушение установленных сроков хранения копий программ и информации, а иногда и полное их отсутствие;

8. отсутствие, несовершенство или отступление от правил эксплуатации программ для компьютерной техники, баз данных и аппаратных средств обеспечения сетевых технологий.

Преступник размещает в информационном пространстве ложную информацию с целью совершения мошенничества или создает специальный сайт в сети Интернет, регистрирует несколько виртуальный номеров у SIP-провайдеров. Анализ такой «фейковой» информации актуален для понимания преступлений в сфере охраняемой законом информации и позволит предупреждать такого рода преступления[1].

Анонимность в сети Интернет также является одним из факторов совершения преступлений в сфере охраняемой законом информации и позволяет осуществлять незаконную деятельность, причем используя при этом возможности сети Интернет, и является препятствием для привлечения к ответственности виновных лиц, так как возможности проведения оперативно-розыскных мероприятий и следственных действий ограничены, ввиду отсутствия сил и средств на территориях других государств и малоэффективного международного сотрудничества. А так как технологии предоставляют возможность, находясь в России, пускать свой трафик через любую другую страну, проблем становится еще больше.

---

[1] *Родивилин И.П., Родивилина В.А.* Информационное оружие // Материалы Международного Байкальского форума Евразийский интеграционный проект: цивилизационная идентичность и глобальное позиционирование». 2018. С. 276.

Также хочется отметить, что средства шифрования препятствуют доступу к содержимому, даже при перехвате данных, так как их расшифровка требует значительных технических ресурсов и времени.

Технология блокчейн, а в частности криптовалюта, предоставляют возможность совершать платежи вне государственного регулирования, и помогает скрывать личность в сети Интернет.

Средства анонимности, в том числе браузер «TOP», распространяются бесплатно и открыто, любой желающий может их установить и пользоваться ими, что способствует анонимизации пользователей.

Наиболее криминализованной частью сети Интернет является «Даркнет» (Darknet), представляющий собой небольшой сегмент так называемого «глубинного Интернета» (Deep Web), под которым понимается разнообразный контент, недоступный большинству поисковых систем. В «Даркнете» все скрывается от общедоступных поисковых механизмов абсолютно осознанно. Так, информация в нем спрятана с помощью специального программного обеспечения, обеспечивающего шифрование и анонимность пользователей, использующего домены и протоколы, на которые среднестатистический интернет-пользователь никогда не натолкнется.

Анонимная сеть – это сегмент, где можно узнать практически любую информацию и купить множество товаров. Данная среда представляет собой частные сети, которые используют лишь доверенные соединения, важнейшая характерная черта которых – полная анонимность. В связи с этим отследить пользователя в этой сети практически невозможно. Данный факт способствовал развитию в «Даркнете» нелегального бизнеса.

Ни один поисковый механизм либо браузер, кроме «TOP», не предоставляют желающим доступ к ресурсам «Даркнета». Своеобразным путеводителем по анализируемому сегменту выступает «скрытая Википедия» (Hidden Wiki), представляющая собой каталог ссылок на скрытые ресурсы, находящиеся не на привычных доменах (к примеру, .ru, .com, .biz и т.д.), а на псевдо-домене «.onion».

Ссылки «Даркнета» представляют собой хаотичный набор букв и цифр, а вход на многие сайты зачастую осуществляется или после регистрации, или после ввода найденного на специальных форумах пароля.

На «Hidden Wiki» можно найти продавцов оружие, наркотиков, краденой электроники, детской порнографии. Так на популярной торговой площадке «HYDRA» в категориях товара можно найти: марихуану, каннабиноиды, стимуляторы, эйфоретики, психоделики, экстази, диссоциативы, опиаты, конструкторы (они же составляющие для сбора приборов и дальнейшего синтеза каких-либо наркотических средств, например мефедрона), в категории «аптека» можно найти различные медицинские препараты, свободный оборот которых запрещен, SSH и VPN, а в цифровых товарах размещены услуги по компьютерному шпионажу, взлому мессенджеров WhatsApp и Telegram, код-граберы, «пробивы» по различным базам данным (в том числе базы ГИБДД, Сбербанка, ВТБ24, базам организаторов радиоподвижной связи – Tele2, МТС, Билайн, Мегафон и т.д.), «взлом» различных аккаунтов, услуги по блокировкам банковских карт, узнавания баланса и кодового слова, а также роутеры, ноутбуки и планшеты со встроенным шифрованием), в «документах» можно приобрести сканы паспортов, купить новый паспорт, как Российский, так и иностранного государства, оформить заграничный или служебный паспорт, дипломы среднего профессионального и высшего образования, изготовление различных печатей, справок, различные бланки государственных образцов, удостоверение сотрудника МВД, водительские удостоверения и др., в категории «карты и сим» предоставляется различные банковские карты, идентифицированные QIWI-кошельки и «анонимные» сим-карты, фальшивые деньги, приборы и оборудования для производства и сбыта наркотиков и майнинговые «фермы», анаболические стеройды и даже вакансии на, так называемых «кладменов», курьеров, складчиков, трафаретчиков.

Облегченное приобретения данных веществ и предметов значительно затрудняет, а то и вовсе лишает возможности выявления первоначального произво-

дителя и поставщика, в результате чего, даже при установлении личности продавца или сбытчика, освободившееся место тут же занимает другой.

Также можно найти сайты, представляющие собой инструкции для педофилов с подробным описанием всех нюансов педофилии и форумы – поддержки и обсуждения данной темы.

«Даркнет», в основном, англоязычен, однако имеются в нем и локальные сайты. Русскоязычный сегмент приютил множество магазинов, торгующих контрабандной черной икрой, краденой электроникой, фальшивыми долларами, паспортами и государственными номерами. Одна из подобных площадок носит название Russian Road.

Немалый простор «Deep Web» предоставляет финансовым сервисам, посредством которых можно очень быстро улучшить свое материальное состояние. Здесь можно приобрести краденые аккаунты платежной системы «PayPal», аппараты для копирования пластиковых карточек, «отмыть» биткоины. Отдельная графа занята коммерческими сервисами, предлагающими купить краденую технику, к примеру, «разблокированные» телефоны марки «iPhone» за треть рыночной стоимости. Такими «универмагами» предлагаются поддельные докторские степени, оборудование для производства наркотиков, оформление эмиграции и др.

Помимо рассмотренных, в «Даркнете» существуют сегменты, в которых полную волю предоставляют себе люди с серьезными психическими аномалиями, религиозные секты, разномастные вербовщики и много другое.

Вместе с тем, невзирая на обладание высоким уровнем защиты сеть «TOP» имеется немало уязвимостей, позволяющих отследить пользователя и передаваемую им информацию. «TOP» предназначается для сокрытия факта связи между сервером и клиентом, однако он принципиально не способен обеспечить полное сокрытие передаваемых данных, так как в данном случае шифрование выступает только средством достижения анонимности в сети Интернет. Известно, что для сохранности более высокого уровня конфиденциальности требуется дополни-

тельная защита самих коммуникаций. Кроме этого значимо шифрование файлов, передаваемых посредством «TOP», с помощью упаковки таковых в криптографические контейнеры, а также применение методов стеганографии.

Методы, принимаемые для установления личности преступников в «Deep Web», достаточно ограничены и осложнены особенностями данной сети. Так, для поиска преступников используют:

1. Анализ имеющихся данных. Данный метод основан на том, что человек не может быть предельно внимательным при осуществлении какой – либо деятельности и может допускать небольшие ошибки или же просто что-то забыть. А для торговых площадок – имеется необходимость привлечения клиентов, для чего используются общедоступные сети. Так, например, проведение наблюдений, спецопераций и ОРМ осуществляемых специальными техническими подразделениями правоохранительных органов разных стран позволяют установить точки соприкосновения реального и виртуального миров.

2. Перехват почтовых отправлений, в России – ОРМ «Контроль почтовых отправлений, телеграфных и иных сообщений». Заключается в том, что правоохранительные органы тесно сотрудничают с почтовыми компаниями и могут исследовать подозрительные отправления, получать данные об отправителе или получателе.

3. Внедрение информационных систем, обрабатывающих большие объемы данных. «Кто владеет информацией – тот владеет миром», так говорил Натан Ротшильд, первостепенное значение информация имеет и для борьбы с преступностью. Так введение информационных систем, обладающих искусственным интеллектом и возможность дальнейшего самообучения позволяют устанавливать связи, которые человек обычным анализом установить бы не смог (использование IP-адресов, анализ историй активности, сопоставление пользователей по вторичной информации и сведениях).

4. Отслеживание денежных потоков. Хотя использование криптовалюты затрудняет деанонимизацию владельца, а то и вовсе делает её невозможным, сла-

бым местом здесь выступает покупка и продажа цифровой валюты. Правоохранительные органы различных стран имеют правомочия отправлять запросы в биржи биткоина, чтобы узнать информацию о том, кто и где совершал сделки по покупке или продаже криптовалюты. Наиболее известным решением в сфере мониторинга незаконного оборота биткоина – Eliptic, проект, который сотрудничает с финансовыми институтами и правоохранительными органами.

5. Оперативное внедрение технического плана, без непосредственного контакта, через интернет. Заключается в попытке входа в доверие к администраторам запрещенных сайтов, изображая розничных и оптовых продавцов.

6. Взлом и использование модифицированного программного обеспечения. Заключается во внедрении технологических решений исходя из использования уязвимостей сайтов или сетей с целью пересылки IP-адресов пользователей и иных данных, которые могут помочь в идентификации преступных элементов. Сюда можно отнести различные специальные оперативно-розыскные мероприятия технического характера, предусмотренные ФЗ «Об ОРД».

Безусловно, анализируемая область социальных отношений крайне своеобразна и проблемна. Перечень упомянутых недостатков в законодательной и практической сферах противодействия использованию анонимности в криминальных целях не исчерпывающий. Для эффективного противодействия прежде всего необходимо развитие технических возможностей по доступу к необходимой информации, эффективное сотрудничество на международном уровне и грамотное использование имеющихся сил и средств.

Организационные факторы. Часто безответственное отношение руководителей к вопросу обеспечения информационной безопасности и защите информации, приводит к неправомерному доступу к охраняемой законом информации. К упущениям организационного характера можно отнести: неконтролируемый доступ сотрудников и обслуживающего персонала к внутренней сети организации; низкий профессионализм или отсутствие служб информационной безопасности, отсутствие должностного лица, отвечающего за

режим секретности и конфиденциальность информации; отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения конфиденциальной информации; недостаточное финансирование мероприятий по защите информации. Непродуманная кадровая политика в вопросах приема на работу и увольнения.

Низкий уровень специальной подготовки должностных лиц правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере обращения охраняемой законом информации. В ходе проведенного опроса, 55 % респондентов (сотрудники специализированных подразделений по борьбе с преступлений в сфере информационных технологий) признались, что им не хватает знаний в сфере информационной безопасности, информационных технологий.

Социально-экономические факторы. Огромные финансовые потоки в нелегальных видах интернет-бизнеса скрыты от государства, это приводит к тому, что все они остаются «в тени» без правового и социального контроля, тем самым снижая риски быть пойманными. На наш взгляд, данное обстоятельство формирует в киберпространстве условия, при которых появляется возможность получения преступным путем сверхприбыли при минимальных затратах и рисках.

Возможность получения сверхприбыли при минимальных затратах и минимальном риске является объективным детерминантом преступности в сфере оборота охраняемой законом информации, поскольку побуждает виновных их совершать. Данную проблему, на наш взгляд, можно решить профилактикой киберпреступности среди населения и популяризацией легальных способов получения крупных доходов в сети Интернет.

Усиление цифрового неравенства между странами запада и России является одной из причин появления преступлений в сфере компьютерной информации[1]. Под цифровым неравенством понимается, с одной стороны, «различие в уровнях

[1] *Родивилин И.П.* Цифровое неравенство – угроза безопасности Российской Федерации // Материалы Международной научно-практической конференции «Проблемы обеспечения национальной безопасности в контексте изменения геополитической ситуации». 2017. С. 140.

развития информационных коммуникаций между различными странами и регионами, внутри страны, возрастными и социальными группами, различными государственными учреждениями, между институтами гражданского общества»[1]; с другой – как разрыв в возможностях доступа к информации между богатыми и бедными (в том числе качественные различия), что характерно и для развитых стран[2].

Так, например, лицензионное программное обеспечение в России стоит относительно дорого и для подавляющего большинства российских пользователей не является проблемой использование контрафактных программ. По рыночным законам спрос рождает предложение, что обуславливает появление создателей специфического вида программного обеспечения под названием «Варез» или «Warez» (от английского «software» – «программное обеспечение»). Указанная общность людей осуществляет распространение программного обеспечения в несколько раз дешевле лицензионного аналога, а в большинстве случаев совершенно бесплатно. Для того, чтобы лицензионная программа стала бесплатной ее нужно «взломать», то есть использовать вредоносную компьютерную программу, заведомо предназначенную для нейтрализации средств защиты компьютерной информации. Такие действия подпадают под признаки состава преступления, предусмотренного ст. 273 УК РФ.

Также стоит обратить внимание на то обстоятельство, что в контрафактном программном обеспечении в большинстве случаев присутствуют вредоносные компьютерные программы. Устанавливая, к примеру, нелицензионный «Windows», пользователь может стать частью сети «Ботнет», то есть на компьютер пользователя будет скрытно установлено программное обеспечение, позволя-

---

[1] *Гиляревский Р.С.* Информатика как наука об информации: информационный, документальный, технологический, экономический, социальный и организационный аспекты / Р.С. Гиляревский. М.: Фаир-Пресс, 2006. С. 304.

[2] *Вальвачев В.В.* Динамика цифрового неравенства в современном мире // Научные проблемы гуманитарных исследований. 2010. №7. URL: http://cyberleninka.ru/article/n/dinamika-tsifrovogo-neravenstva-v-sovremennom-mire.

ющее злоумышленнику выполнять различные действия, используя инфицированный компьютер, например, для совершения ddos-атак.

Еще одно проявление цифрового неравенства заключается в небрежном отношении к цифровой информации, выражающемся в установлении простых паролей для защиты информации и нарушении сроков их использования, либо вообще в отсутствии средств защиты цифровой информации. «Компьютерная система, которую взламывает хакер, не существует сама по себе. Она всегда содержит в себе еще одну составляющую: человека»[1]. Отсутствие знаний по защите информации, обусловлено ограниченным доступом к информационному пространству. Хочется обратить внимание на то обстоятельство, что увеличивается цифровой разрыв между информационными преступниками и их жертвами, что также влияет на количество совершенных преступлений в сфере обращения охраняемой законом информации.

В «Стратегии национальной безопасности Российской Федерации до 2020 года» также отмечаются возросшая «уязвимость всех членов международного сообщества перед лицом новых вызовов и угроз». На основании оценки тенденций развития современного мира и России в документе делается вывод: «Усилится глобальное информационное противоборство, возрастут угрозы стабильности индустриальных и развивающихся стран мира, их социально-экономическому развитию и демократическим институтам»[2]. Таким образом, сокращение цифрового неравенства позволит Российской Федерации не проиграть в информационной войне.

Цифровое неравенство является сложным социально-экономическим понятием, имеющим множество форм проявления. По мнению некоторых ученых, в

---

[1] *Кузнецов М.В.* Социальная инженерия и социальные хакеры / М. В. Кузнецов. СПб.: БХВ-Петербург, 2007. С. 200.

[2] Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы (проект) // scrf.gov.ru Официальный сайт Совета Безопасности Российской Федерации URL: http://www.scrf.gov.ru/documents/6/136.html.

преодоление цифрового неравенства начинается с обеспечения юридически равных возможностей для осуществления права на доступ к сети Интернет[1].

Сокращение цифрового неравенства остается приоритетным направлением деятельности правительства Российской Федерации. Сократив информационный разрыв, возможно решить несколько проблем современного российского общества. Во-первых, сократится оборот нелицензионного программного обеспечения, что сократит преступность в сфере обращения охраняемой законом информации, сократится число «зараженных» устройств, используемых в сетях «Ботнет». Во-вторых, разработка собственного программного обеспечения минимизирует риск получения информации иностранными спецслужбами. В-третьих, повышение рейтинга российских информационных агентств позволит сократить иностранную информационную пропаганду. Информационная безопасность страны не может считаться только государственным или только частным приоритетом. Она затрагивает интересы и простых граждан, и бизнесменов, и государственных служащих. Каждый из нас в равной степени несет ответственность за свободу и будущее нашей страны. Сокращение информационного неравенства до условно допустимых пределов, определяемых уровнем развития социума в целом, всегда будет являться одной из важнейших задач, стоящих перед любым обществом.

Виктимологические факторы. Отыскать жертву в сети Интернет очень легко, ведь пользователи часто при обращении с информацией пренебрегают элементарными требованиями по ее защите, среди которых наиболее часто встречающими являются:

– не уничтожают файлы, содержание информацию ограниченного доступа, с компьютеров общего пользования; наделяют нескольких лиц правом доступа к любым компонентам сети;

– устанавливают сетевые серверы в общедоступных местах;

---

[1] *Туликов А.В.* Информационная безопасность и права человека в условиях постиндустриального развитая (теоретико-правовой анализ): дис. ... канд. юрид. наук. М., 2017. С. 46.

– небрежно хранят записи паролей; используют упрощенные пароли, устанавливаемые для защиты информации в сети Интернет.

Ежегодно из-за утечек персональной информации в сеть Интернет попадают миллионы паролей пользователей. Компания SplashData каждый год составляет список самых простых паролей. Обычно в их отчете оказываются пароли вроде 123456, но каждый год в этом списке появляются и новые позиции – например, в 2018 г. туда попал donald[1]. Между тем пользователи информации пренебрегают сменой пароля от своих учетных записей при разводе, увольнении, потере телефона или записной книжки, тем самым подвергая свою информацию ограниченного доступа опасности неправомерного использования со стороны бывшего супруга, коллеги и т.п.

Фактическая безнаказанность лиц, совершивших преступления в сфере обращения охраняемой законом информации, из-за высокой латентности данных противоправных деяний, отсутствие надлежащей подготовки сотрудников правоохранительных органов, осуществляющих производство по уголовным делам данной категории преступлений[2].

В ходе изучения особенности лиц, ставших жертвой преступления в сфере обращения охраняемой законом информации, получены следующие выводы: мужчины становились жертвами преступлений в 58,6% случаев, а женщины – в 41,4%. В Российской интернет-аудитории приблизительно такое же соотношении полов[3]. Средний возраст потерпевшего около 34 лет, что на 4 года больше среднего возраста пользователя Интернет в России.

Как и жертвы неправомерного доступа, потерпевшие в результате компьютерного мошенничества в большинстве случаев (70,3%) не знакомы с жертвой. Такие особенности Интернета, как анонимность и возможность доступа из любой

---

[1] Worst Passwords of 2018 // teamsid.com. URL: https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018.
[2] *Мерзлов Ю.А*. Указ. соч. С. 57.
[3] Интернет в цифрах и фактах // compress.ru. URL: http://compress.ru/article.aspx?id=14772/

точки мира, позволяют мошенникам совершать преступления в масштабах всей планеты и против граждан любой страны.

Пренебрежение средствами компьютерной защиты носит повсеместный характер. Таким образом, основным виктимологическим фактором является несоблюдение потерпевшим мер информационной безопасности.

Основываясь на вышесказанном, жертвами преступников, специализирующихся на преступлениях в сфере оборота охраняемой законом информации могут стать: лица независимо от пола, в возрасте от 18 до 34 лет, доверчивые, являющиеся активными пользователями электронных кошельков и (или) систем дистанционного банковского обслуживания (Онлайн-банки), с низкой культурой информационной безопасности, как правило, пользователи мобильных устройств, пренебрегающие средствам компьютерной защиты (антивирусами) либо использующие контрафактные средства защиты.

Определяющее значение имеет деятельность государства в лице уполномоченных органов по разработке и регламентации общегосударственных вопросов защиты Российского информационного пространства, выявлению и устранению обстоятельств, способствующих посягательствам на охраняемую законом информацию. При этом необходимо учитывать влияние как внешних, так и внутренних факторов, способствующих количественному росту рассматриваемых преступлений.

Не исключено, что в скором времени проблема информационной безопасности и защиты данных станет в один ряд с такими глобальными проблемами современности, как экологический кризис, коррупция, отсталость развивающихся стран и др.

На основании вышеизложенного можно сделать вывод, что существование преступности в сфере оборота охраняемой законом информации определяются несколькими специфическими факторами, которые не совпадают с факторами, порождающими преступность в целом. К таким факторам можно отнести:

– факторы правового характера (отсутствие механизма регулирования сети Интернет; отсутствие единого понятийного аппарата при определении преступлений, совершенных в сфере обращения охраняемой законом информации, отсутствие уголовной ответственности за ограничение доступа к охраняемой законом информации);

– технические факторы (рост числа устройств, подключенных к сети Интернет, увеличение объемов информации, недостаточность защиты самих технических устройств; анонимность пользователей сети Интернет);

– организационные факторы (неконтролируемый доступ сотрудников к внутренней сети организации; низкий профессионализм или отсутствие служб информационной безопасности; недостаточное финансирование мероприятий по защите информации; низкий уровень специальной подготовки должностных лиц правоохранительных органов, которые должны предупреждать, раскрывать и расследовать преступления в сфере обращения охраняемой законом информации);

– социально-экономические факторы (возможность получения сверхприбыли при минимальных затратах и минимальном риске при совершении преступлений в сфере оборота охраняемой законом информации; усиление цифрового неравенства);

– виктимологические факторы (небрежность в работе пользователей информации, их неосмотрительное поведение, выражающееся в установлении простых паролей для защиты информации и нарушении сроков их использования, либо отсутствие средств защиты информации, а также знаний по защите информации).

ГЛАВА 4. ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ В СФЕРЕ ОБРАЩЕНИЯ ОХРАНЯЕМОЙ ЗАКОНОМ ИНФОРМАЦИИ

§ 1. Уголовно-правовые меры предупреждения преступлений в сфере обращения охраняемой законом информации

Проблема противодействия преступлениям, совершаемым в сфере оборота охраняемой законом информации, продолжает оставаться одной из наиболее злободневных.

Следует согласиться с мнением, что рассмотрение вопросов преступности, факторов ее детерминирующих, личности преступника является основой для понимания процессов борьбы с преступностью и предупреждения преступности[1]. Рассмотренные выше уголовно-правовая и криминологическая характеристики преступлений в сфере обращения охраняемой законом информации позволяют сформулировать основные направления противодействия преступности в указанной сфере на современном этапе развития Российской Федерации.

Значение противодействия преступлениям сложно переоценить. Понятие противодействия преступлениям многогранно и представляет собой деятельность государственных органов, институтов гражданского общества, организаций и физических лиц, направленную против преступных посягательств, целью которой является выявление причин и условий, способствующих осуществлению противоправной деятельности, а также минимизации и ликвидации последствий противоправной деятельности[2].

В УК РФ уже сформирована система норм, устанавливающих уголовную ответственность за посягательства на неприкосновенность и сохранность

---

[1] *Репецкая А.Л., Рыбальская В.Я*. Криминология: Часть Общая: учебное пособие. Иркутск, 1999. С. 62.

[2] Майоров А.В. Понятие и структура системы противодействия преступности // Правопорядок: история, теория, практика. 2014. №1 (2). URL: http://cyberleninka.ru/article/n/ponyatie-i-struktura-sistemy-protivodeystviya-prestupnosti.

охраняемой законом информации, но она нуждается в дальнейшей оптимизации сообразно новым вызовам информационного общества.

В науке криминологии определяют противодействие как комплекс взаимоувязанных социально-экономических, политических, культурно-воспитательных мер, осуществляемых государственными, муниципальными органами, общественными формированиями и отдельными гражданами[1]. К этим мерам необходимо добавить технические и организационные меры, так как они также вносят огромный вклад в противодействие преступлениям в сфере обращения охраняемой законом информации, в силу их специфики.

Противодействие преступлениям в сфере обращения охраняемой законом информации будет слабым без глубокого понимания правовых проблем регулирования информационного пространства. Давно назрела необходимость в совершенствовании отечественного уголовного законодательства, в том числе норм уголовного кодекса Российской Федерации, регламентирующих ответственность за преступления в сфере обращения охраняемой законом информации, а также норм в сфере регулирования сети Интернет, что явилось бы эффективной правовой мерой борьбы как с преступность в сфере обращения охраняемой законом информации, так в целом с компьютерной преступностью.

Представляется верным утверждение Ю.В. Добрынина о том, что для последующего предотвращения противоправных деяний, а также предупреждения сложности выбора статей, по которым необходимо предъявлять обвинения по данным преступлениям, необходимо совершенствовать законодательство РФ с целью внесения точности и ясности в нестабильные вопросы компьютерного права в России[2].

Борьбу с подобного рода преступлениями затрудняет отсутствие соответствующего преступления в УК РФ, предусматривающего ответственность за блокировку интернет-ресурсов посредством DdoS-атак. Для противодействия

---

[1] *Воронин Ю А*. Введение в криминологию: курс лекций. М., 2008. 103 с.

[2] *Добрынин Ю.В.* Классификация преступлений в сфере компьютерной информации // www.russianlaw.net Право и Интернет URL: http://law/computer_crime/a158.

описанным преступлениям, наносящим огромный вред экономике государства, необходимо совершенствовать российское законодательство.

Рассматривая DdoS-атаку с технической точки зрения, правоприменителю понятна и ясна схема ее совершения, однако с позиции уголовно-правового понимания этого явления возникает ряд трудностей. По сложившейся практике DdoS-атака квалифицируют по совокупности двух статей Уголовного кодекса Российской Федерации: ст. 272 (неправомерный доступ к компьютерной информации) и ст. 273 (создание, использование и распространение вредоносных компьютерных программ).

Например, *Саянским городским судом Иркутской области вынесен приговор в отношении гр. М., который осуществлял DdoS-атаки на сайты в сети Интернет. Гр. М. приобрел VDS-сервер, на котором располагалась панель управления ботнет-сетью. После чего, изучив принцип работы приобретенного VDS-сервера, осознавая, что данная программа предназначена для организации DDoS-атак на удаленный ресурс в сети Интернет, то есть нарушению нормального функционирования интернет-сайта и компьютерной техники, на котором расположен сайт, путем их блокирования, он внес изменения (модифицировал) на данном сервере и установил программу «DRAGON», которая представляла собой набор необходимых файлов, скриптов (сценариев), написанных на языке «PHP», а также файлов, написанных на языке разметки HTML, предназначенных для создания единой административной панели, базирующейся на веб-сервере. Данная административная панель представляет интерфейс для учета, просмотра, назначения заданий для специализированного программного обеспечения, устанавливаемого на удаленные компьютеры, которые обозначаются словом «бот» («ботами»), с ее помощью назначались задания, которые выполнялись специализированным программным обеспечением на удаленных компьютерах. В дальнейшем, гр. М. скопировал с сайта в сети Интернет на свой компьютер вредоносную программу под названием «Loader.exe». В последующем, у гр. М. возник умысел на организацию DDoS-атак*

на различные интернет-ресурсы. В целях получения денежного вознаграждения, для осуществления незаконной деятельности, направленной на несанкционированное блокирование доступа легальных пользователей сети Интернет к информации, содержащейся на различных Интернет ресурсах (сайтах, доменах), посредством проведения DDoS-атак, осуществляемых в результате распространения и при помощи использования им в сети Интернет вредоносных программ, гр. М. разместил в сети Интернет информацию о предоставлении услуг по осуществлению DDoS-атак за денежное вознаграждение. Затем, получив на персональный компьютер сообщение со стороны неустановленного лица, использовавшего в интернет-системе мгновенного обмена текстовыми сообщениями ICQ, в котором его попросили произвести DDOS-атаку. Обговорив с заказчиком сумму заказа равную 100 долларам США, получив указанные денежные средства на кошелек «Webmoney», за денежное вознаграждение, указанный заказчиком IP-адрес, гр. М. поместил в поле ввода адреса для атаки, выбрал тип атаки – micro flood. В дальнейшем, гр. М., в целях несанкционированного блокирования доступа легальных пользователей сети Интернет к информации, содержавшейся на интернет-ресурсах, отправил команду на начало DDoS-атаки. Указанные выше вредоносные программы, действуя скрытно для пользователей компьютеров, входивших в состав каждой ботнет-сети, инициировали аномально большое количество TCP-соединений (SYN-Flood), отправку аномально большого количества HTTP GET запросов, а также отправку аномально большого количества сетевых пакетов по протоколам UDP и ICMP на интернет-ресурс, что привело к блокированию информации, размещенной на указанном интернет-ресурсе, для доступа легальных пользователей сети Интернет[1].

При рассмотрении данного уголовного дела, суд квалифицировал действия гр. М. по отправке аномального количества запросов на интернет-ресурс как неправомерный доступ к компьютерной информации, однако осуществленная гр.

[1] Архив Саянского городского суда Иркутской области, 2014 г., уголовное дело № 1-14/2014.

М. DdoS-атака на интернет-ресурс с использованием вредоносных компьютерных программ не подпадает под диспозицию указанной статьи.

Как уже было рассмотрено выше, под неправомерным доступом к охраняемой законом информации понимается незаконное либо неразрешенное владельцем или иным ее законным владельцем использование возможности получения информации. Закон предусматривает под доступом к информации возможность получения информации и ее использования. Другими словами, доступ к информации можно считать осуществленным с момента, когда пользователь выполнил некоторые действия, в результате которых стало возможным получать и использовать информацию, ранее для пользователя недоступную. Также под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее)[1].

Если же речь идет о DdoS-атаке на интернет-ресурс, то проникновения в ее источник не происходит. Другими словами, злоумышленник не получает доступ к управлению сайтом и не может использовать администраторские права для блокировки доступа к информации, находящейся на сервере. Таким образом, в данном случае неправомерного доступа, с точки зрения уголовного права не происходит.

Уголовно-правовым аспектом DdoS-атак в Российской Федерации занимались ряд ученых, среди которых И.Г. Чекунов, полагающий, что назрела необходимость введения нового состава преступления – «неправомерное воздействие на функционирование системы» (преднамеренное неправомерное деяние, направленное на отказ в обслуживании компьютера, компьютерных систем или их сети, осуществляемое с использованием протоколов межсетевого

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М., 2013. С 18.

взаимодействия, с целью прекращения или создания задержек обработки сетевых запросов) – DOS (DI-DOS) атаки[1].

В юридической литературе существуют высказывания о необходимости включения в состав ряда преступлений (ст. ст. 146, 160, 165, 183, 189 УК РФ и т.д.) такой способ их совершения, как «применение компьютерных средств». Так, например, А.Б. Попов предлагает сформулировать диспозицию ч. 1 ст. 183 УК РФ как «собирание сведений, составляющих коммерческую, налоговую или банковскую тайну, путем похищения документов, подкупа или угроз, путем перехвата в средствах связи, незаконного доступа к охраняемой законом информации, использования специальных технических средств, а равно иным незаконным способом»[2].

К.Н. Евдокимов предлагает ввести в качестве квалифицирующего признака формулировку «...с применением компьютерной информации, ЭВМ, системы ЭВМ, сети ЭВМ, системы или сети связи, иных высокотехнологичных и научно-технических средств»[3].

Е.А. Лысак считает правильным ввести квалифицирующий признак «совершение преступления с использованием информационных технологий» в ряд статей УК РФ[4]. Нельзя не согласиться с этим мнением, ввиду того, что введение квалифицирующего признака в составы преступлений способно облегчить квалификацию и доказывание преступлений, совершаемых с использованием охраняемой законом информации ограниченного доступа.

Вторая группа ученых считает целесообразным введение отдельной главы или раздела, посвященного компьютерным преступлениям. Например,

---

[1] *Чекунов И.Г.* Криминологические и уголовно-правовые аспекты предупреждения киберпреступлений. Российский следователь. 2013. №3. С. 43.

[2] *Попов А.Б.* Проблемы квалификации преступлений в сфере компьютерной информации // Вестник ТГУ. 2008. № 10 (66). С. 339–344.

[3] *Евдокимов К.Н.* Вопросы уголовно-правовой квалификации неправомерного доступа к компьютерной информации и его отграничения от смежных составов преступлений // Вестник Академии Генеральной прокуратуры РФ. 2009. № 10. С. 42–46.

[4] *Лысак Е.А*. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ. № 90 (06). 2013. С. 727.

С.С. Шахрай предлагает создать в рамках IX раздела УК РФ «Преступления против общественной безопасности и общественного порядка» самостоятельную главу 28-1 «Информационные преступления» и значительно расширить перечень компьютерных преступлений[1].

М.А. Ефремова разделяет эту позицию и считает возможным включение в УК РФ нового раздела «Преступления против информационной безопасности»[2]. Небезупречным представляется и данный подход, ввиду того что компьютерные преступления посягают на различные объекты, среди которых личность, ее честь и достоинство, собственность, экономическая деятельность, общественная безопасность и т.д. Если же говорить о введении нового раздела в УК РФ, то здесь встает вопрос о соблюдении принципа системности уголовного законодательства. Кроме того, до сих пор ни на международном, ни на национальном уровне зарубежных государств, не прекращаются дискуссии об определении примерного перечня компьютерных преступлений. Поэтому, на наш взгляд, прежде чем говорить о введении нового раздела в УК РФ, необходимо определить и уточнить содержание видов преступлений, совершаемых с использованием информационных технологий. Например, предлагается включить в УК РФ такие преступления, как компьютерный саботаж, компьютерный шпионаж, кибертерроризм. Эту позицию поддерживает Хурум М.А. и считает, что нет целесообразности в выделении самостоятельной главы, которая объединила бы нормы о преступлениях, связанных с получением и разглашением информации, вследствие выраженной неоднородности общественных отношений, с которыми связана та или иная информация[3].

Против расширения ИТ-статей в УК РФ выступает и бывший начальник Бюро Специальных Технических мероприятий МВД России Мирошников Б.Н., одной из задач которого является выявление и раскрытие преступлений,

---

[1] *Шахрай С.С.* Система преступлений в сфере компьютерной информации: автореф. дис. … канд. юрид. наук. М., 2010. С. 10.
[2] *Ефремова М.А*. Указ.соч. С. 51.
[3] *Хурум М.А*. указ. соч. С. 121.

совершенных в сфере обращения охраняемой законом информации. Он аргументирует свою позицию тем, что преступные схемы с использованием информационных технологий и сети Интернет с каждым днем совершенствуются и границ тут нет, поэтому не нужно применять излишнюю детализацию и систематизацию УК РФ[1].

При совершении ddos-атаки на сайт в сети Интернет пользователи санкционировано обращаются на сайт, но хотя и владельцы компьютерной техники этого не осознают, сайт фактически для этого и создан, чтобы на него заходили пользователи.

Другой пример, если злоумышленник специально приобрел несколько тысяч компьютеров, с целью того что они совершали аномальное количество обращений на определенный сайт в сети Интернет, с целью совершить ddos-атаку, то привлечь его к уголовной ответственности в настоящий момент не получиться ввиду отсутствия соответствующей нормы в уголовном кодексе РФ. Однако право граждан на доступ к информации, закрепленное в Конституции РФ будет нарушено, а собственник информационного ресурса не сможет распространять свою услуги или информацию. Вся информационная безопасность государства подвергается опасности, если ddos-атаки будут совершаться на сайты государственных органов и компаний. Под незаконным ограничением доступа к информации, находящейся в телекоммуникационных сетях, следует понимать нарушение права граждан на получение информации, свободу распространения информации законным способом.

В связи с вышеизложенным предлагается дополнить УК РФ статьей 274^2 следующего содержания:

«Статья 274^2 Незаконное ограничение доступа к информации.

1. Незаконное ограничение доступа к информации, находящейся в телекоммуникационных сетях», –

---

[1] Борис Мирошников: Сетевой фактор. Интернет и общество // labirint.ru. URL: labirint.ru/books/494759.

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору, организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или из корыстной заинтересованности, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления, –

В главе 28 Уголовного кодекса Российской Федерации устанавливается ответственность только за неправомерный доступ к компьютерной информации, хотя как было описано в первом параграфе первой главы настоящего исследования, компьютерная информация является лишь частью охраняемой законом информации. Таким образом наряду с компьютерной информацией, названой в ст. 272 Уголовного кодекса Российской Федерации, целесообразно будет включить все виды охраняемой законом информации. Тем самым совершенствуется закон, произойдет отказ от спорной практики отнесения информации к охраняемой законом через ее нахождение в определенном устройстве или способе передачи и обработки, как уже ранее произошло исключение термина машинный носитель и ЭВМ из диспозиции ст. 272 УК РФ. Тем самым будет учтены все носители и устройства,

на которых хранится и которыми обрабатывается информация, на что обращают внимание некоторые ученые и постоянно предлагают вносить новые устройства, в которых циркулирует информация[1].

Таким образом, предлагаем статью 272 УК РФ изложить в следующей редакции:

«Статья 272 Неправомерный доступ к информации

1. Неправомерный доступ к охраняемой законом информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода, осужденного за период до восемнадцати месяцев, 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.

Кроме того, необходимо закрепить в УК РФ следующие понятия, которые были рассмотрены выше во 2 параграфе:

1. Неправомерный доступ к охраняемой законом информации.
2. Блокирование охраняемой законом информации.
3. Модификация охраняемой законом информации.
4. Копирование охраняемой законом информации.
5. Ограниченнее доступа к информации, расположенной в сети Интернет.
6. Охраняемая законом информация ограниченного доступа.

Часть первую статьи 273 изложить в следующей редакции:

«Создание, распространение или использование компьютерных программ либо иной информации, заведомо предназначенных для несанкционированного

---

[1] См. *Бегишев И.Р.* Указ. соч. С. 9-40.

ознакомления, уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты информации, –».

Ч.1 ст. 274 УК РФ изложить в следующей редакции:

«Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой законом информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее ознакомление, уничтожение, блокирование, модификацию либо копирование информации, причинившее крупный ущерб, – »

наказываются лишением свободы на срок до семи лет.

Подобные меры противодействия преступлениям в сфере охраняемой законом информации помогут снизить их рост, оперативнее выявлять виновных лиц, совершающих преступления подобной категории.

Обозначенные уголовно-правовые меры, в совокупности, способны устранить сложности при квалификации преступлений в сфере обращения охраняемой законом информации, декриминализировать действия по неправомерному доступу к охраняемой законом информации, хотя и имеющие признаки преступления, но в силу отсутствия вредных последствий, не несущие опасности для общества.

§ 2. Иные специальные криминологические меры предупреждения преступлений в сфере обращения охраняемой законом информации

Рассмотрение в исследовании поставленных уголовно-правовых и криминологических проблем в конечном результате имеет целью предупреждение преступности. Методы противодействия преступлениям должны соответствовать современным реалиям. Преступления в сфере обращения охраняемой законом информации постоянно пополняются новыми способами совершения, новой техни-

кой, устройствами. В этой связи необходимо поменять подход к профилактике и борьбе с преступлениями в данной сфере. Для осуществления эффективной работы правоохранительных органов необходимо создание системы предупреждения рассматриваемых преступлений.

Со стороны государства проблеме противодействия в сфере обращения охраняемой законом информации уделяется внимание, о чем свидетельствует включение этой проблемы в основные цели Концепции общественной безопасности Российской Федерации. Однако принимаемых мер в настоящий момент недостаточно.

Исходя из факторов совершения преступлений в сфере обращения охраняемой законом информации, предлагаются следующие специально-криминологические меры противодействия указанным видам преступлений.

Проведенный анализ уголовных дел о преступлениях в сфере обращения охраняемой законом информации, исследование особенностей их совершения, данные о личности преступника и потерпевшего позволили выделить ряд задач, выполнение которых качественно улучшит профилактическую работу правоохранительных органов по борьбе с преступлениями в сфере обращения охраняемой законом информации.

Во-первых, необходимо включить сайты, на которых происходит общение лиц, интересующихся преступления в сфере обращения охраняемой законом информации в реестр запрещённых сайтов, на ряду с порнографическими сайтами, сайтами по пропаганде наркотиков и т.д. Под влиянием негативного информационного потока и обещания быстрого обогащения и совершения преступлений в сфере обращения охраняемой законом информации у лица может возникнуть мотив для совершения преступления. Другими словами, сайт в сети Интернет является отправной точкой для запуска механизма преступного поведения.

При этом не нужно забывать и о том, что предупреждение – это машина, включающая в себя большое количество механизмов, среди которых уголовно-правовые средства должны стоять не на первом месте, исходя из идеи, что совер-

шение деяния должно быть предупреждено, а не наказано. Если каким-либо пользователям сети Интернет удалось обойти блокировку сайта, то необходимо, не дожидаясь от него конкретных, реальных действий, воплощающих его умысел, проводить профилактическую беседу. Таким образом, блокировка подобного рода сайтов и контроль их посетителей будет является эффективным способом предупреждения преступлений в сфере обращения охраняемой законом информации.

По нашему мнению, в целях противодействия таким преступлениям и всем киберпреступлениям в целом, в Российской Федерации в первую очередь необходимо принять Национальную Стратегию кибербезопасности. В данной Стратегии должны быть сконцентрированы все нормы, регулирующие общественные отношения, связанные с сетью Интернет, охраняемой законом информацией, закрепленные в настоящий момент в различный подзаконных актах, а иногда в локальных актах коммерческих организаций. В некоторых таких положениях содержатся нормы, применение которых позволило сократить риск совершения преступлений в сфере обращения охраняемой законом информации и облегчить поиск злоумышленников.

Также хочется добавить еще одно немаловажное свойство сети Интернет – ее наднациональность, то есть Интернет по его сути не является продуктом какого-либо отдельного государства и в связи с этим конкретное государство не имеет возможности осуществлять контроль за всем киберпространством.

Следует обратить внимание на то обстоятельство, что дать отпор преступлениям в сфере обращения охраняемой законом информации в частности и киберпреступлениям в целом невозможно без международного сотрудничества и принятия международных соглашений в области противодействия преступлениям в сфере обращения охраняемой законом информации. С.В. Воронцова считает, что «отдельная страна не может самостоятельно вести борьбу с киберпреступностью и только международное сообщество способно

противостоять данному виду преступности»[1]. Решить проблему могло бы тесное взаимодействие следователей и оперативных работников, занимающихся выявлением, раскрытием преступлений в сфере обращения охраняемой законом информации.

Тем не менее, большинство стран неохотно раскрывают сведения о банковских счетах своих граждан, например, США и страны Европейского Союза. Сложившаяся международная обстановка, способствует изоляции России от внешнего мира. Это является неоправданным шагом, так как российские граждане в большинстве случает, являются субъектами совершения преступления, а не потерпевшими. А вот иностранцы становятся жертвами российских хакеров и непредоставление информации российским правоохранительным органам, в первую очередь, наносит вред их безопасности.

Для предупреждения трансграничных преступлений, к которым можно отнести и значительную часть преступлений в сфере обращения охраняемой законом информации, немаловажная роль отведена государствам, и только при хорошо скоординированной работе правоохранительных органов различных стран возможно снизить количество совершаемых правонарушений в рассматриваемой сфере. Важно отметить, что традиционные механизмы международного сотрудничества, применяемые в 20 веке, являются неподходящими в эру, когда преступления могут совершаться из любой точки земного шара со скоростью света[2].

Сложность выработки международных актов в целом в рассматриваемой ситуации осложняется еще и тем, что «существующие законы трудно применять,

---

[1] *Воронцова С.В*. Киберпреступность: проблемы квалификации преступных деяний. Российская юстиция. 2011. №2. С. 14-15.

[2] *Smith R.G.* Criminals on Trial / R.G. Smith, P. Grabosky, G. Urbas. – Cambridge University Press, 2004. – P. 60.

когда речь идет о неподдающихся локализации атаках в планетарных масштабах, доказательства которых разбросаны и виртуальны»[1].

Анонимность киберпространства – это основной принцип его существования. Все пользователи сайтов, форумов или социальных сетей в киберпространстве изначально не имеют ни имён, ни внешнего вида – они эфемерны, и нередко информационные ресурсы сами присваивают таким пользователям имя «anonymous», то есть аноним. Выбрать имя и внешний вид сайты предлагают каждому своему пользователю самостоятельно и в подавляющем большинстве случаев пользователи злоупотребляют такой возможностью, представляясь чужими именами и используя чужие фотографии.

Зарегистрировавшись под чужим именем, любой может безнаказанно обманывать, совершать анонимные платежи и переводы денежных средств, совершать хищения, вымогательства и иные экономические киберпреступления. Действующие способы вычисления виновных способны установить точное место, откуда виновный совершил вход в киберпространство, с точностью до квартиры, и приблизительную личность виновного, включая его национальную принадлежность, однако в самом киберпространстве существуют тысячи способов скрыть свою личность. Это подтверждают материалы судебной практики, где всё чаще используются такие формулировки как «неустановленное лицо», «в неустановленное время», «в неустановленном месте», «с неустановленного компьютера» и т.д.

Однако на сегодняшний день существует механизм, благодаря которому государство получает возможность осуществлять регулирование в сети Интернет, хотя и не совсем достаточное для ограничения роста преступности, используя технические меры противодействия преступлениям в сфере обращения охраняемой законом информации. Как правило, при совершении противоправного деяния, злоумышленники пытаются обезопасить себя и используют разные

---

[1] *Жилина И.Ю.* Киберпреступность и борьба с ней (сводный реферат) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 2, Экономика: реф. журн. 2003. № 1. С. 144.

способы для того, чтобы остаться анонимными в виртуальном пространстве. Существует много способов сохранить анонимность – анонимайзеры[1], проксисервер[2], сеть «TOP» и т.д. Однако существует и более простой и доступный способ скрыть свою личность в глобальной паутине – воспользоваться пунктом коллективного доступа к сети Интернет. Это можно сделать двумя способами. Первый, воспользоваться бесплатным Wi-Fi-соединением в кафе, ресторанах, вокзалах, аэропортах и т.д. Второй, воспользоваться услугами интернет-кафе и за небольшую плату, без предъявления каких-либо документов, войти в сеть Интернет.

Доступу к Wi-Fi-соединению в местах общего доступа государство в последнее время уделяет внимание, например, принято Постановление Правительства РФ от 31 июля 2014 г. № 758 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей» (далее – Постановление Правительства РФ № 758)[3]. Внесенные изменения гласят, что теперь оператором связи должна осуществляться идентификация пользователей сети Интернет через установление фамилии, имени и отчества (если оно имеется), которые подтверждаются паспортом или иным документом,

---

[1] Средство для скрытия информации о компьютере или пользователе в сети Интернет. Может быть программой, устанавливаемой на компьютер.

[2] От англ. proxy – право пользоваться от чужого имени, удаленный компьютер, который, при подключении к нему используемого компьютера, становится посредником для выхода абонента в интернет. Прокси-сервер передает все запросы программ абонента в сеть, и, получив ответ, отправляет его обратно абоненту.

[3] О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»: Постановление Правительства РФ от 31 июля 2014 г. № 758 // Собрание законодательства Российской Федерации. – 2014. – № 32 – Ст. 4525.

удостоверяющим личность. Кроме того, установление личности пользователя возможно «иным способом, обеспечивающим достоверное установление указанных сведений». Оператор вправе выбирать, как именно осуществлять идентификацию пользователя. Он может отправить пользователю запрос на получение идентификационных данных при помощи СМС-сообщения или предложить специальную форму для указания данных перед открытием доступа в сеть Интернет. Либо, если на компьютерном устройстве нет СИМ-карты, определить устройство по ID и один раз запросить у пользователя персональные данные при входе в сеть Интернет, как обычно делается, когда доступ имеет пароль. И пользователь обязан предоставить любую идентификационную информацию, например, имя, фамилию и отчество, номер водительского удостоверения и так далее.

Однако, несмотря на то, что уже несколько лет назад вступило в законную силу Постановление Правительства РФ № 758, механизм реализации его мер на практике так и не установлен. Более того, многие владельцы коллективных точек доступа в сеть Интернет до сих пор не знакомы с разъяснениями Министерства связи и массовых коммуникаций Российской Федерации.

В изменениях в Правилах оказания услуг связи Постановлением Правительства РФ № 758 не сказано, что идентификация пользователей коллективных точек доступа Wi-Fi обязательно должна происходить только через мобильные номера российского оператора. Запрета нет, это очевидно. Но иностранные сотовые операторы информацию о владельце номера телефона могут и не дать. На сайте государственных услуг иностранные граждане тоже не зарегистрированы. Для удостоверения личности иностранец может предъявить паспорт администрации общественного места, где установлена точка доступа к Wi-Fi; оформить СИМ-карту российского оператора связи и авторизоваться с ее помощью.

С технической точки зрения организовать доступ к сети Интернет в общественных местах по документу, удостоверяющему личность или с привязкой

к телефонному номеру не сложно. Для этого следует организовать так называемый гостевой доступ, для получения которого на специальной web-страничке заполнить специальную форму. Помимо фамилии и имени можно затребовать и дополнительные требования, например, номер мобильного телефона или адрес электронного почтового ящика. После создания учетной записи пользователь должен получить логин и пароль (если включить режим доступа по логину/паролю, а не доступ без регистрации). Сделать это возможно следующими способами: распечатать на принтере и принести гостю вместе с меню; отправить на электронный почтовый ящик (для этого у гостя должен быть доступ к нему); направить реквизиты доступа посредством СМС-сообщений.

Если для пользования пунктами коллективного доступа по Wi-Fi в общественных местах законодательная база есть, хотя и механизм четко не проработан, то интернет-кафе остается привлекательным местом для киберпреступников. Во многих странах, действуют жесткие меры идентификации лиц, пользующих подобного рода услугами. Так, например, в Китае посетителей интернет-кафе обязали предоставлять администрации документы – паспорт или удостоверение личности. В свою очередь владельцы кафе обязаны четко регистрировать кто, когда и за каким компьютером выходил в сеть Интернет.

Владельцы интернет-клубов в Белоруссии несут ответственность за сообщения посетителей. Если IP-адрес, который выделялся при совершении какого-либо противоправного деяния ведет в интернет-кафе, имеется возможность привлечь к ответственности его владельца. Таким образом, владелец пункта доступа к сети Интернет по Wi-Fi становится первым заинтересованным лицом, в том, чтобы в клубе были видеокамеры, учет пользователей, логирование посещений[1].

Власти Италии приняли закон, согласно которому владельцы точек публичного доступа в сеть Интернет обязаны копировать паспорта клиентов и

---

[1] Владельцы интернет клубов в Белоруссии несут ответственность за сообщения посетителей // internet-club.info. URL: http://internet-club.info/node/50.

отслеживать сайты, которые они посещают, а также устанавливать специальные программы для слежения за активностью клиентов. Генерируемые программой отчеты регулярно должны направляться в полицию. Также отмечается, что перлюстрации переписки подвергаются только те лица, которые находятся в «черных списках» правоохранительных органов[1].

В Казахстане каждого посетителя снимают на видеокамеру, данные должны храниться в базе заведения не менее шести месяцев, клиентам необходимо с собой иметь всегда документ, удостоверяющий личность. Детям и подросткам, не достигшим 16 лет, не запрещено посещать общественные пункты доступа к сети Интернет, но при посещении интернет-клубов они будут обязаны предъявить официально выданную учебным заведением справку с вклеенной фотографией[2].

Оператор связи обязан хранить информацию об абонентах и оказанных им услугах связи, а также иной информации, необходимой для выполнения возложенных на уполномоченные органы задач в течение 3 лет[3]. Федеральный закона «О связи», возлагает на операторов связи обязанность по хранению информации о фактах приема, передачи, доставки и (или) обработки голосовой информации, текстовых сообщений, изображений, звуков, видео- или иных сообщений пользователей услугами связи – в течение трех лет с момента окончания осуществления таких действий. И действительно, операторы связи хранят в установленном порядке эти сведения и предоставляют их по запросу компетентных органов.

Анализ работы оперативных сотрудников и следователей свидетельствует о том, что успех их деятельности по раскрытию и расследованию преступлений в сфере охраняемой законом компьютерной информации, наряду с другими

---

[1] Итальянские интернет-кафе начали ксерокопировать паспорта клиентов // lenta.ru. URL: https://lenta.ru/news/2005/10/05/cafe.

[2] *Аккулы С.Х.* В интернет-клуб можно теперь зайти только с паспортом // azattyq.org. URL: http://rus.azattyq.org/a/internet_cafe_restictions _kazakhstan/24478911.html.

[3] Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» // Собрание законодательства Российской Федерации. – 2005. – № 36. – Ст. 3704.

факторами, в определенной мере зависит от своевременного предоставления операторами связи информации об абоненте, которому выделялись IP-адреса в интересующее время[1].

В этой связи, хочет обратить внимание на проблему, так называемых, «серых» IP-адресов, то есть публичные сетевые адреса, преобразованные по технологии NAT (Network Address Translation). Благодаря этой технологии один IP-адрес может быть одновременно предоставлен нескольким абонентам или устройствам, количество которых может доходить до нескольких тысяч. Так как большинство преступлений в сфере обращения охраняемой законом информации возможно раскрыть лишь благодаря получению сведений от оператора связи о владельце IP-адреса, с использованием которого было совершено преступление, то сетевые адреса, преобразование по технологии NAT, затрудняют работу правоохранительных органов по выявлению и раскрытию преступлений.

Технология NAT позволяет преступникам безнаказанно совершать все новые и новые преступления, в виду сложности их изобличения. Операторы связи в своей работе применяют Internet Protocol (IP) версии IPv4, который использует 32-битные адреса, ограничивающие адресное пространство 4 294 967 296 уникальными адресами и этих адресов уже на всех абонентов и устройств не хватает. По причине постоянного увеличения пользователей и ограниченности сетевой адресов, операторы связи прибегают к технологии NAT, которая внедряется достаточно просто.

Протоколу Ipv4 имеется альтернатива интернет протокол IPv6, который предусматривает наличие 340,000,000,000,000,000,000,000,000,000,000,000,000 уникальных адресов[2]. Внедрение нового протокола может способствовать борьбе с преступлениями в сфере обращения охраняемой законом информации, в силу

---

[1] *Родивилин И.П., Коломинов В.В., Брыжак Д.Э.* Интеллектуальный разврат несовершеннолетних в сети Интернет // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. № 1. С. 72.

[2] *Хазов В*. Все, что вам надо знать о разнице между IPv4 и IPv6 // vasexperts.ru URL: http://blog.vasexperts.ru/?p=815.

более точного выявления абонента, оставляющего электронные следы в сети Интернет.

Таким образом, предлагаем на законодательном уровне обязать операторов связи использовать интернет протокол Ipv6 по предоставлению телекоммуникационных услуг на территории Российской Федерации и полностью отказаться от технологии NAT.

В результате экспертного опроса было выявлено, что факты совершения преступлений в сфере обращения охраняемой законом информации были выявлены следующим образом:

– в результате регулярных проверок организаций собственными службами коммерческой безопасности – 31%;

– в результате агентурной работы, а также при проведении оперативных мероприятий по проверкам заявлений граждан – 28%;

– случайно – 18%;

– в ходе проведения налоговых, бухгалтерских ревизий – 13%;

– в ходе расследования других видов преступлений – 10%.

Путями преодоления латентности преступлений в сфере обращения охраняемой законом информации можно назвать следующие.

1. Использование социологических методов и приемов выявления и измерения латентной преступности в сфере высоких технологий: массовый опрос населения, анкетирование, экспертные оценки, анализ материалов средств массовой информации.

2. Использование экономико-правовых методов, основанных на анализе всех взаимосвязанных технико-экономических показателей деятельности хозяйствующих субъектов.

3. Преодоление правового нигилизма руководителей учреждений, предприятий, организаций и отдельных граждан путем освещения проблем компьютерной преступности в средствах массовой информации. Необходимо обратить внимание общества на те возможные негативные последствия, которые содержит в себе

угроза роста латентной преступности в сфере обращения охраняемой законом информации.

4. Обеспечение законности функционирования системы уголовной юстиции в государстве, повышение уровня доверия населения к ней.

5. Пересмотр статистического подхода к изучению компьютерной преступности, что, безусловно, повлечет за собой снижение латентности данного вида преступлений.

6. Повышение эффективности правоохранительной деятельности, требовательности к уровню профессионализма работников правоохранительных органов. В связи с этим необходимо введение спецкурсов по изучению проблем компьютерной преступности в юридических вузах нашего государства.

7. Дальнейшая работа по совершенствованию законодательной базы в сфере охраны информации, так как она, безусловно, влечет за собой снижение уровня латентности данного вида преступных посягательств.

Необходимо информировать граждан о соблюдении информационной безопасности, используя популярные интернет-ресурсы, телевидение и т.п. Повышая информационную грамотность, снижается риск стать жертвой преступления в сфере обращения охраняемой законом информации. Ведь «Компьютерная система, которую взламывает хакер, не существует сама по себе. Она всегда содержит в себе еще одну составляющую: человека».[1] Согласно проведенным исследованиям внешние атаки стали причиной 33% утечек данных, где в 67% случаев утечка данных произошла под воздействием внутреннего нарушителя, а в 1% случаев – высшие руководители организаций[2].

Обязательно осуществление координации деятельности правоохранительных органов и иных органов и организаций в целях профилактики борьбы с преступлениями в сфере обращения охраняемой законом информации. В частности,

---

[1] *Кузнецов М.В.* Указ.соч. С. 10

[2] Глобальное исследование утечек конфиденциальной информации в I полугодии 2016 года // infowatch.ru. URL: https://www.infowatch.ru/sites/default/files/report/analytics/russ /InfoWatch_Global_Report_2016_ half_year.pdf?rel=1.

нуждается в укреплении взаимодействие правоохранительных органов и операторов связи для оперативного получения у них информации об абонентах и оказанных им услугах связи. Нужно сформировать рабочие группы, состоящие из представителей органов местного самоуправления, студентов, лиц, занимающих информационной безопасностью и возложить на них обязанность по мониторингу сети Интернет с целью отыскания потерпевших от преступлений в сфере обращения охраняемой законом информации, а также о лицах, осуществляющих подобного рода деятельность.

Также необходимо повышать эффективность работы правоохранительных органов, организовывать межрегиональное сотрудничество на территории Российской Федерации, а также межгосударственное взаимодействие.

Снижению уровня латентности преступлений в сфере обращения охраняемой законом информации, на наш взгляд способствует подготовка компетентных сотрудников с достаточным уровнем знаний в сфере информационных технологий, а также взаимодействие со средствами массовой информации.

Следует проводить индивидуальное предупреждение, которое включает в себя работу с лицами, склонными к совершению преступлений в сфере обращения охраняемой законом информации, в целях предотвращения их криминальной самореализации.

Правительство Российской Федерации разработало документ под названием «Основные направления деятельности Правительства Российской Федерации на период до 2018 года», в котором делается акцент на проведение работы по устранению цифрового неравенства посредством развития широкополосного доступа к сети «Интернет». Однако на сегодняшний день по скорости Интернета Россия занимает в мире лишь 47 место[1]. По развитию информационно-коммуникационных

[1] State of the internet // akamai.com. URL:https://www.akamai.com/us/en/multimedia/documents/report/q3-2015-soti-connectivity-final.pdf.

технологий в мире Россия в 2015 году занимала 45 место[1]. Также, Российская Федерация в 2016 году занимала 7 строчку по числу пользователей Интернета 103147691 человек, это составляет 70,5 % от общего населения страны. В США этот показатель в процентном соотношении больше и равен 88,6 % от населения страны[2].

Со всей уверенностью можно сказать, что сейчас имеются практически все условия для защиты домашних компьютеров и корпоративных сетей от несанкционированного доступа.

Активными мерами в борьбе с этим видом преступлений будет является разработка и внедрение системы виктимологической профилактики интернет-преступлений. Во-первых, важно создать систему мер правовой пропаганды и повышения уровня правосознания граждан. Во-вторых, выстроить эффективную криминологическую профилактику, направленную на повышение технического уровня пользователей с учетом соответствующей аудитории: интернет-пользователей, которые не используют средства защиты или не знают о существовании таковых, и профессиональных пользователей, которым необходимо получать информацию о новых внедрениях в сфере компьютерной безопасности. Рекомендуемые средства защиты должны ранжироваться в зависимости от ценности защищаемых компьютерных данных и навыков пользователя.

По этой причине противодействие преступлениям в сфере обращения охраняемой законом информации должно включать в себя следующие направления:

1. Постоянный мониторинг лиц, склонных к совершению преступлений в сфере обращения охраняемой законом информации, который необходимо возложить на специальные подразделения органов внутренних дел. Стоит обратить внимание, что эта деятельность в основном должна проводиться в виртуальной среде.

---

[1] Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы (проект) // scrf.gov.ru Официальный сайт Совета Безопасности Российской Федерации URL: http://www.scrf.gov.ru/documents/6/136.html.

[2] TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS // internetworldstats.com. URL: http://www.internetworldstats.com/top20.htm.

2. Осуществление административного надзора за лицами, допускающими совершение правонарушений и преступлений в сфере обращения охраняемой законом информации.

Пользователи сети Интернет, хоть и выступают каждый сам за себя, все же формируют виртуальные социальные сообщества, которые могут рассматриваться как «новая устойчивая форма существования социальных отношений»[1].

В этой связи необходимо разработать систему максимально полного информирования правоохранительными органами граждан, в том числе и посредством подготовки информационных материалов по проблемам преступлений, посягающих на охраняемую законом информацию.

С учетом того, что жертва такого преступления в большинстве случаев отказывается заявлять в правоохранительные органы из-за убеждения в отсутствии результата и недоверия к полиции, необходимо повышать уровень доверия к полиции населения через достижение высоких стандартов полицейской деятельности, повышение уровня взаимодействия с общественностью и других показателей.

Ввиду отсутствия четких границ по защите персональных и пользовательских данных в российском законодательстве и включение цифровых прав человека в Конституцию РФ, пользователи сети Интернет в настоящий момент должны сами позаботиться о своей безопасности в сети Интернет:

1. Шифрование всех данных. Даже если компьютерная система защищена паролем, злоумышленник сможет легко сбросить его, загрузившись с внешнего диска. Сбрасывать пароль также не нужно – любой Live-дистрибутив Linux может легко прочитать и скопировать данные. Поэтому, нужно предпринять меры по шифрованию информации.

2. Использование менеджеров паролей, который генерирует каждый раз новые случайные пароли для любого создаваемого аккаунта в сети Интернет.

---

[1] *Манойло А.В*. Объекты и субъекты информационного противоборства // piter.com. URL: http://psy.piter.com/Hbrary/?tp=1&rd=8&l=636&p=1293.

Абсолютная приватность в сети Интернет недостижима в принципе. Но перечисленные приёмы смогут защитить пользователей сети Интернет от кражи конфиденциальных данных мошенниками, от любопытства коллег, сидящих за одним столом, от назойливого внимания маркетологов Google и Microsoft.

Внимание к данной проблеме и активная работа в обозначенных направлениях являются, на наш взгляд, важным шагом на пути эффективного выявления и предупреждения преступлений, в сфере обращения охраняемой законом информации.

Методы противодействия преступлениям должны соответствовать современным реалиям. Преступления в сфере обращения охраняемой законом информации постоянно пополняются новыми способами совершения преступлений, новой техникой, устройствами. На данном этапе необходимо поменять подход к профилактике и борьбе с преступлениями в данной сфере.

Формулируя выводы, следует отметить, что для предупреждения преступлений в сфере обращения охраняемой законом информации наиболее действенными представляются меры специально-криминологического предупреждения, которые можно разделить на следующие группы:

1. Правовые меры (предложение о включении в УК РФ понятия неправомерного доступа к охраняемой законом информации, а также понятия общественно-опасных последствий в виде блокирования, модификации, копирования и ограничения доступа к охраняемой законом информации).

2. Технические (реализация комплекса мер по борьбе с анонимностью пользователей в сети Интернет; введение информационных систем, обрабатывающих большие объемы данных; создание информационной базы данных о вредоносных компьютерных программах; использование операторами связи интернет-протокола Ipv6 по предоставлению телекоммуникационных услуг на территории Российской Федерации с полным отказом от технологии NAT).

3. Организационные (налаживание должного государственного регулирования за пунктами коллективного доступа в сеть Интернет; включение в

реестр запрещённых сайтов специфических интернет-ресурсов, на которых происходит обмен информацией о способах совершения преступлений в сфере обращения охраняемой законом информации; подготовка компетентных сотрудников правоохранительных органов с достаточным уровнем знаний в сфере информационных технологий).

4. Социально-экономические (отслеживание денежных потоков в сети Интернет (в том числе взаимодействие с интернет-биржами по обмену криптовалют на другие средства платежа); борьба с цифровым неравенством).

5. Виктимологические (информирование граждан о необходимости и способах соблюдения информационной безопасности, через популярные интернет-ресурсы, телевидение; повышение технического уровня пользователей сети Интернет).

ЗАКЛЮЧЕНИЕ

Итоги выполненного исследования. Проведенное диссертационное исследование уголовно-правовых и криминологических проблем противодействия преступлениям в сфере обращения охраняемой законом информации в полной мере позволило раскрыть криминологическую характеристику преступлений в сфере обращения охраняемой законом информации, решить поставленные задачи и достичь цели исследования.

Результаты диссертационного исследования выявили текущее состояние, динамику и структуру преступлений в сфере обращения охраняемой законом информации, уточнили и дополнили предложения, рекомендации по совершенствованию уголовного законодательства и иных нормативно-правовых актов по вопросам, связанным с совершением преступлений в сфере обращения охраняемой законом информации, обозначили уголовно-правовые и криминологические меры противодействия преступлениям в сфере обращения охраняемой законом информации и привели нас к следующим выводам.

В исследовании доказано, что в качестве предмета необходимо употреблять термин «охраняемая законом информация», поскольку он является более широким по сравнению с компьютерной информацией, а так же электронной или цифровой. Такая необходимость обуславливается тем, что в УК РФ должен охранять общественные отношения в сфере обращения информации ограниченного доступа, а объект уголовно-правовой охраны не должен ограничиваться только компьютерной информацией. Принимая во внимание, что охраняемая законом информация может быть зафиксирована на цифровом носителе, может размещаться в информационно-телекоммуникационных сетях, а также на бумажном носителе, нет необходимости специально выделять в отдельную группу объектов преступлений общественные отношения, возникающие в сфере обращения информация ограниченного доступа.

Учитывая вышесказанное, под преступлением в сфере обращения охраняемой законом информации предложено понимать виновно совершенное общественно опасное деяние, посягающее на общественные отношения, возникающие по поводу охраны информации ограниченного доступа. При этом можно выделить главные свойства информации: владелец информации предпринял действия по защите информации; информация подпадает под сведения ограниченного доступа, режим оборота которой регулируется Конституцией РФ или федеральными законами. Преступления в сфере обращения охраняемой законом информации можно классифицировать в зависимости от способа совершения противоправного деяния. При этом выделяются следующие группы: использование вредоносных компьютерных программ для мобильных телефонов, неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам, кардинг, скимминг, ddos-атака.

Появился новый вид преступлений в сфере обращения охраняемой законом информации Вэб-кардинг, за который редко подвергаются уголовному наказанию, как правило, это происходит, когда преступник и потерпевший находятся на территории Российской Федерации[1]. Низкий уровень взаимодействия между правоохранительными органами различных государств затрудняет процесс противодействия вэб-кардингу. Необходима разработка и реализация стратегии международного сотрудничества в сфере противодействия компьютерной преступности.

От общественно-опасных последствий неправомерного доступа к охраняемой законом информации и использования вредоносных компьютерных программ в виде копирования и модификации следует отграничивать модификацию и копирование метаданных, то есть информацию об использовании информации, поскольку эти действия не охватываются умыслом преступника и происходят в независимости от его действий, и не наносят вред обладателю информации. Также

---

[1] *Родивилин И.П.* Уголовно-правовое и криминологическое противодействие вэб-кардингу // Библиотека уголовного права и криминологии. 2017. № 1(19). С. 128.

в УК РФ необходимо закрепить понятия блокирование, модификация, уничтожение охраняемой законом информации.

Преступления в сфере обращения охраняемой законом информации в большинстве случаев образуют реальную совокупность преступлений с другими общественно-опасными деяниями, посягающими на один предмет – охраняемую законом информацию ограниченного доступа, но при этом имеют разные основные непосредственные объекты. В этой связи, верным представляется утверждение о том, что необходимо квалифицировать подобные деяния по нескольким составам Особенной части УК РФ, оценивая общественную опасность каждого преступления.

Вышеизложенное свидетельствует о том, что существующее уголовное законодательство в области противодействия преступлениям в сфере обращения охраняемой законом информации, далеко несовершенно, хоть и прошло двадцатилетний путь становления.

Изучение особенностей лиц, совершающих преступления, является важным условием правильной организации борьбы с определенным видом преступной деятельности. Для преступлений в сфере обращения охраняемой законом информации, изучение личности преступника приобретает особую актуальность, так как в данном случае речь идет о субъектах, которые до недавнего времени не попадали в поле зрения правоохранительных органов.

Круг лиц, совершающих преступления в сфере обращения охраняемой законом информации, не ограничивается только «хакерами». К лицам, совершающим преступления в сфере электронной информации, следует применять термин «информационные воры», так как их целью является похищение важного в современном мире ресурса – информации. Информационные воры являются частью отдельной категории преступников, которых принято называть киберпреступниками.

Современные преступники, специализирующиеся на преступлениях в сфере обращения охраняемой законом информации, не являются одиночками, а

собираются в группы. На просторах Интернета имеется обилие ресурсов, объединенных едиными убеждениями – совершать преступления в киберпространстве. Следует обратить внимание на то обстоятельство, что участники организованной группы в большинстве случаев никогда не встречались друг с другом лицом к лицу и проживают в разных регионах мира. Все общение между ними происходит с использованием информационных средств коммуникации через сеть Интернет, практически всегда с использованием программного обеспечения, позволяющего анонимно общаться в киберпространстве. Информационные воры – это не Робин Гуды, они работают из корыстной заинтересованности, однако иногда встречаются лица с психическими отклонениями или совершающие преступления с целью проверить свои навыки.

Рекомендации и перспективы дальнейшей разработки темы исследования. Опасность преступлений в сфере оборота охраняемой законом информации обусловлена тем, что современные информационно-телекоммуникационные технологии, ворвавшись в нашу жизнь, стали ее неотъемлемой составляющей и преобразовали индустриальный социум в информационное общество. Цифровой прорыв вызвал всплеск новых угроз информационной безопасности, порожденных глобализацией информационных процессов.

Однако с момента принятия действующего УК РФ нормы об ответственности за рассматриваемые преступления практически не пересматривались и не дополнялись, что привело к пробелам в уголовном законодательстве.

Учитывая быстрое развитие информационных технологий, необходимо ставить перед разработчиками программного обеспечения, производителями оборудования, службами, занимающимися информационной безопасностью, и другими структурами вопросы о предотвращении возможностей для совершения преступлений в сфере обращения охраняемой законом информации. Методы противодействия преступлениям должны соответствовать современным реалиям.

Преступления в сфере обращения охраняемой законом информации постоянно пополняются новыми способами совершения преступлений, новой техникой, устройствами. На данном этапе необходимо поменять подход к профилактике и борьбе с преступлениями в данной сфере.

В связи с тем, что проблема защиты информации находится в спектре приоритетных направлений Российской Федерации, то назрела необходимость в государственном регулировании за пунктами коллективного доступа в сети Интернет, что не позволит киберпреступникам скрывать свою личность и облегчит выявление лиц, совершающих преступления в сфере обращения охраняемой законом информации. Также со стороны государства требуется ввести административную ответственность по отношению к владельцам пунктов коллективного доступа в сеть Интернет, которые игнорируют правила авторизации пользователей.

В то же время правоприменительная практика нуждается в содержательных и однозначных разъяснениях уголовного закона, позволяющих решать проблемы, возникающие при квалификации исследуемых деяний, в числе которых определение понятий «охраняемая законом информация» и преступления в сфере ее обращения.

Проведенное исследование показывает, что регламентация рассматриваемых норм несовершенна: имеются неточности в формулировании определений понятий, проблемы и противоречия нормативно-правового регулирования, неудачные решения в описании отдельных составов преступлений в сфере оборота охраняемой законом информации.

Таким образом, представленное монографическое исследование носит целостный и законченный характер и включает в себя комплекс уголовно-правовых и криминологических мер, реализация которых, будет способствовать снижению количества преступлений в сфере обращения охраняемой законом информации, и совершенствованию деятельности правоохранительных органов на этом направлении.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативные правовые акты и иные официальные документы

1. Конституция Российской Федерации от 12 декабря 1993 г.: с учетом правок, внесенных Законами РФ о поправках к Конституции Российской Федерации от 30 декабря 2008 г. № 6-ФКЗ, от 30 декабря 2008 г. № 7-ФКЗ, от 05 февраля 2014 г. № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ // Собрание законодательства Российской Федерации. – 2014. – № 31 – Ст. 4398.

2. Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 № 95-ФЗ: в ред. Федерального закона от 2 декабря 2019 г. № 406-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 30. – Ст. 3012.

3. Бюджетный кодекс Российской Федерации от 31 июля 1998 г. № 145-ФЗ: в ред. Федерального закона от 27 декабря 2019 г. № 479-ФЗ // Собрание законодательства Российской Федерации. – 1998. – № 31. – Ст. 3823.

4. Гражданский кодекс РФ (часть вторая) от 26 января 1996 г. № 14-ФЗ: в ред. Федерального закона от 27 декабря 2019 г. № 489-ФЗ // Собрание законодательства Российской Федерации. – 1996. – №5. – Ст. 410.

5. Гражданский кодекс РФ (часть третья) от 26 ноября 2001 г. № 146-ФЗ: в ред. Федерального закона от 18 марта 2019 г. № 34-ФЗ // Собрание законодательства Российской Федерации. – 2001. – №49. – Ст. 4552.

6. Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ: в ред. Федерального закона от 2 декабря 2019 г. № 406-ФЗ // Собрание законодательства Российской Федерации. – 2002. – №46. – Ст. 4532.

7. Налоговый кодекс Российской Федерации (часть 1) от 31 июля 1998 г. № 146-ФЗ: в ред. Федерального закона от 26 марта 2020 г. № 68-ФЗ // Собрание законодательства Российской Федерации. – 1998. – № 31. – Ст. 3824.

8. Налоговый кодекс Российской Федерации (часть 2) от 05 августа 2000 г. № 117-ФЗ: в ред. Федерального закона от 26 марта 2020 г. № 68-ФЗ // Собрание законодательства Российской Федерации. – 2000. – № 32. – Ст. 3340.

9. Федеральный закон от 02 декабря 1990 г. № 395-1 «О банках и банковской деятельности»: в ред. Федерального закона от 27 декабря 2019 г. № 507-ФЗ // Ведомости съезда народных депутатов РСФСР. – 1990. – № 27. – Ст. 357.

10. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»: в ред. Федерального закона от 29 июля 2018 г. № 256-ФЗ // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. –1993. – №38. – Ст. 1480.

11. Федеральный закон от 20 апреля 1995 г. № 45-ФЗ «О государственной защите судей, должностных лиц правоохранительных и контролирующих органов»: в ред. Федерального закона от 1 октября 2019 г. № 328-ФЗ // Собрание законодательства Российской Федерации. – 1995. – № 17. – Ст. 1455.

12. Федеральный закон от 12 августа 1995 г. №144-ФЗ «Об оперативно-розыскной деятельности»: в ред. Федерального закона от 02 августа 2019 г. № 311-ФЗ // Собрание законодательства Российской Федерации. – 1995. – № 33. – Ст. 3349.

13. Семейный кодекс Российской Федерации от 29 декабря 1995 г. № 223-ФЗ: в ред. Федерального закона от 6 февраля 2020 г. № 10-ФЗ // Собрание законодательства Российской Федерации. – 1996. – №1. – Ст. 16.

14. Федеральный закон от 07 мая 1998 г. № 75-ФЗ «О негосударственных пенсионных фондах»: в ред. Федерального закона от 18 марта 2020 г. № 61-ФЗ // Собрание законодательства Российской Федерации. – 1998. – № 19. – Ст. 2071.

15. Федеральный закон от 25 июля 1998 г. № 128-ФЗ «О государственной дактилоскопической регистрации в Российской Федерации»: в ред. Федерального закона от 1 октября 2019 г. № 328-ФЗ // Собрание законодательства Российской Федерации. – 1998. – № 31. – Ст. 3806.

16. Федеральный закон от 11 июля 2001 г. № 95-ФЗ «О политических партиях»: в ред. Федерального закона от 2 декабря 2019 г. № 423-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 29. – Ст. 2950.

17. Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ: в ред. Федерального закона от 18 февраля 2020 г. № 25-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 52 (часть I). – Ст. 4921.

18. Федеральный закон от 25 января 2002 г. № 8-ФЗ «О Всероссийской переписи населения»: в ред. Федерального закона о от 11 декабря 2018 г. № 463-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 4. – Ст. 252.

19. Федеральный закон от 05 июля 2010 г. № 154-ФЗ «Консульский устав Российской Федерации»: в ред. Федерального закона от 26 июля 2019 г. № 232-ФЗ // Собрание законодательства Российской Федерации. – 2010. – № 28. – Ст. 3554.

20. Федеральный закон от 21 июля 2011 г. № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса»: в ред. Федерального закона от 6 июля 2016 г. № 374-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 30. – Ст. 4604.

21. Федеральный закон от 21 июля 2005 г. № 108-ФЗ «О Всероссийской сельскохозяйственной переписи»: в ред. Федерального закона от 27 июня 2018 г. № 164-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 30. – Ст. 3019.

22. Федеральный закон от 27 июля 2004 г. № 79-ФЗ «О государственной гражданской службе Российской Федерации»: в ред. Федерального закона от 16 декабря 2019 г. № 432-ФЗ // Собрание законодательства Российской Федерации. – 2004. – № 31. – Ст. 3215.

23. Федеральный закон от 20 августа 2004 г. № 119-ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»: в ред. Федерального закона от 7 февраля 2017 г. № 7-ФЗ // Собрание законодательства Российской Федерации. – 2004. – № 34. – Ст. 3534.

24. Федеральный закон от 20 июля 2012 г. № 125-ФЗ «О донорстве крови и ее компонентов»: в ред. Федерального закона от 7 марта 2018 г. № 56-ФЗ // Собрание законодательства Российской Федерации. – 2012. – № 30. – Ст. 4176.

25. Федеральный закон от 07 февраля 2011 г. № 7-ФЗ «О клиринге и клиринговой деятельности»: в ред. Федерального закона от 27 декабря 2019 г. № 484-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 7. – Ст. 904.

26. Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»: в ред. Федерального закона от 18 апреля 2018 г. № 86-ФЗ // Собрание законодательства Российской Федерации. – 2004. – №32. –Ст. 3283.

27. Федеральный закон от 05 апреля 2013 г. № 44-ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»: в ред. Федерального закона от 27 февраля 2020 г. № 27-ФЗ // Собрание законодательства Российской Федерации. – 2013. – №14. –Ст. 1652.

28. Федеральный закон 03 декабря 2012 г. № 230-ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам»: в ред. Федерального закона от 3 августа 2018 г. № 307-ФЗ // Собрание законодательства Российской Федерации. – 2012. – № 50 (часть IV). – Ст. 6953.

29. Федеральный закон от 30 декабря 2004 г. № 218-ФЗ «О кредитных историях»: в ред. Федерального закона от 2 августа 2019 г. № 259-ФЗ // Собрание законодательства Российской Федерации. – 2005. – № 1. – Ст. 44.

30. Федеральный закон от 19 июля 2007 г. № 196-ФЗ «О ломбардах»: в ред. Федерального закона от 2 декабря 2019 г. № 394-ФЗ // Собрание законодательства Российской Федерации. – 2007. – №31. – Ст. 3992.

31. Федеральный закон от 11 ноября 2003 г. № 138-ФЗ «О лотереях»: в ред. Федерального закона от 1 марта 2020 г. № 46-ФЗ // Собрание законодательства Российской Федерации. – 2003. – № 46 (часть I). – Ст. 4434.

32. Федеральный закон от 02 марта 2007 г. №25-ФЗ «О муниципальной службе в Российской Федерации»: в ред. Федерального закона от 16 декабря 2019 г. № 432-ФЗ // Собрание законодательства Российской Федерации. – 2007. – № 10. – Ст. 1152.

33. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: в ред. Федерального закона от 27 декабря 2019 г. № 480-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ст. 3451.

34. Федеральный закон от 17 июля 1999 г. № 176-ФЗ «О почтовой связи»: в ред. Федерального закона от 27 декабря 2019 г. № 478-ФЗ // Собрание законодательства Российской Федерации. – 1999. – № 29. – Ст. 3697.

35. Федеральный закон от 25 декабря 2008 г. № 273-ФЗ «О противодействии коррупции»: в ред. Федерального закона от 16 декабря 2019 г. № 432-ФЗ // Собрание законодательства Российской Федерации. – 2008. – № 52. – Ст. 6228.

36. Федеральный закон от 07 августа 2001 г. № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»: в ред. Федерального закона от 1 марта 2020 г. № 46-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 33. – Ст. 3418.

37. Федеральный закон от 27 июля 2010 г. № 224-ФЗ О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации: в ред. Федерального закона от 3 августа 2018 г. № 310-ФЗ // Собрание законодательства Российской Федерации. – 2010. – № 31. – Ст. 4193.

38. Закон Российской Федерации от 02 июля 1992 г. № 3185-1 «О психиатрической помощи и гарантиях прав граждан при ее оказании»: в ред. Федерального закона от 19 июля 2018 г. № 213-ФЗ // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – №33. – Ст. 1913.

39. Федеральный закон от 22 апреля 1996 г. № 39-ФЗ «О рынке ценных бумаг»: в ред. Федерального закона от 27 декабря 2019 г. № 495-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 17. – Ст. 1918.

40. Федеральный закон от 26 сентября 1997 г. № 125-ФЗ «О свободе совести и о религиозных объединениях»: в ред. Федерального закона от 2 декабря 2019 г. № 407-ФЗ // Собрание законодательства Российской Федерации. – 1997. – № 39. – Ст. 4465.

41. Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»: в ред. Федерального закона от 1 марта 2020 г. № 42-ФЗ // Собрание законодательства Российской Федерации. – 2003. – № 28. – Ст. 2895.

42. Федеральный закон от 30 ноября 2011 г. № 342-ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»: в ред. Федерального закона от 16 декабря 2019 г. № 432-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 49. – Ст. 7020.

43. Федеральный закон от 24 июля 2008 г. № 161-ФЗ «О содействии развитию жилищного строительства»: в ред. Федерального закона от 2 декабря 2019 г. № 401-ФЗ // Собрание законодательства Российской Федерации. – 2008. – № 30. – Ст. 3617.

44. Федеральный закон от 28 декабря 2013 г. № 426-ФЗ «О специальной оценке условий труда»: в ред. Федерального закона от 27 декабря 2019 г. № 451-ФЗ // Собрание законодательства Российской Федерации. – 2013. – № 52. – Ст. 6991.

45. Федеральный закон от 08 декабря 2003 г.№ 165-ФЗ «О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров»: в ред. Федерального закона от 26 июля 2017 г. № 205-ФЗ // Собрание законодательства Российской Федерации. – 2003. – № 50. – Ст. 4851.

46. Закон Российской Федерации от 27 декабря 1991 г. № 2124-1 «О средствах массовой информации»: в ред. Федерального закона от 1 марта 2020 г.

№ 42-ФЗ // Ведомости Съезда народных депутатов Российской Федерации и Верховного Совета Российской Федерации. – 1992. – № 7. – Ст. 300.

47. Федеральный закон от 24 июля 2009 г. № 212-ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»: в ред. Федерального закона от 19 декабря 2016 г. № 438-ФЗ // Собрание законодательства Российской Федерации. – 2009. – № 30. – Ст. 3738.

48. Федеральный закон от 21 июля 1997 г. № 118-ФЗ «Об органах принудительного исполнения Российской Федерации»: в ред. Федерального закона от 27 декабря 2019 г. № 487-ФЗ // Собрание законодательства Российской Федерации. – 1997. – № 30. – Ст. 3590.

49. Закон Российской Федерации от 22 декабря 1992 г. № 4180-1 «О трансплантации органов и (или) тканей человека»: в ред. Федерального закона от 23 мая 2016 г. № 149-ФЗ // Ведомости Съезда народных депутатов РФ и Верховного Совета Российской Федерации. – 1993. – № 2. – Ст. 62.

50. Федеральный закон от 09 февраля 2007 г. № 16-ФЗ «О транспортной безопасности»: в ред. Федерального закона от 2 декабря 2019 г. № 415-ФЗ // Собрание законодательства Российской Федерации. – 2007 – № 7. – Ст. 837.

51. Федеральный закон от 24 июля 2002 г. №102-ФЗ «О третейских судах в Российской Федерации»: в ред. Федерального закона от 28 ноября 2018 г. № 451-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 30. – Ст. 3019.

52. Федеральный закон от 10 июля 2002 г. № 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»: в ред. Федерального закона от 18 марта 2020 г. № 50-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 28. – Ст. 2790.

53. Федеральный закон от 07 декабря 2011 г. № 414-ФЗ «О центральном депозитарии»: в ред. Федерального закона от 6 февраля 2020 г. № 7-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 50. – Ст. 7356.

54. Федеральный закон от 31 мая 2002 г. № 63-ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»: в ред. Федерального закона от 2 декабря 2019 г. № 400-ФЗ // Собрание законодательства Российской Федерации. – 2002. – № 23. – Ст. 2102.

55. Федеральный закон от 15 ноября 1997 г. № 143-ФЗ «Об актах гражданского состояния»: Федеральный закон (в ред. Федерального закона от 1 октября 2019 г. № 328-ФЗ // Собрание законодательства Российской Федерации. – 1997. – № 47. – Ст. 5340

56. Федеральный закон от 27 июля 2010 г. № 193-ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)»: в ред. Федерального закона от 26 июля 2019 г. № 197-ФЗ // Собрание законодательства Российской Федерации. – 2010. – № 31. – Ст. 4162.

57. Федеральный закон от 30 декабря 2008 г. № 307-ФЗ «Об аудиторской деятельности»: в ред. Федерального закона от 26 ноября 2019 г. № 378-ФЗ // Собрание законодательства Российской Федерации. – 2009. – № 1. – Ст. 15.

58. Федеральный закон от 28 ноября 2011 г. № 335-ФЗ «Об инвестиционном товариществе»: в ред. Федерального закона от 27 декабря 2018 г. № 514-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 49. – Ст. 7013.

59. Федеральный закон от 29 ноября 2001 г. № 156-ФЗ «Об инвестиционных фондах»: в ред. Федерального закона от 2 декабря 2019 г. № 394-ФЗ // Собрание законодательства Российской Федерации. – 2001. – № 49 – Ст. 4562.

60. Федеральный закон от 01 апреля 1996 г. № 27-ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»: в ред. Федерального закона от 24 апреля 2020 г. №

136-ФЗ // Собрание законодательства Российской Федерации. – 1996. – № 14. – Ст. 1401.

61. Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защиты информации»: в ред. Федерального закона от 3 апреля 2020 г. № 105-ФЗ // Собрание законодательства Российской Федерации. 2006. – № 31. – Ст. 3448.

62. Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»: в ред. Федерального закона от 24 апреля 2020 г. № 147-ФЗ // Собрание законодательства Российской Федерации. 2006. – № 53. – Ст. 7598.

63. Федеральный закон от 10 июня 2008 г. № 76-ФЗ «Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания»: в ред. Федерального закона от 27 декабря 2018 г. № 528-ФЗ // Собрание законодательства Российской Федерации. – 2008. – № 24. – Ст. 2789.

64. Федеральный закон от 29 ноября 2010 г. № 326-ФЗ «Об обязательном медицинском страховании в Российской Федерации»: в ред. Федерального закона от 24 апреля 2020 г. № 147-ФЗ // Собрание законодательства Российской Федерации. – 2010. – № 49. – Ст. 6422.

65. Федеральный закон 24 июля 1998 г. № 125-ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»: в ред. Федерального закона от 01 апреля 2020 г. № 102-ФЗ // Собрание законодательства Российской Федерации. – 1998. – № 31. – Ст. 3803.

66. Федеральный закон от 21 ноября 2011 г. № 325-ФЗ «Об организованных торгах»: в ред. Федерального закона от 27 декабря 2019 г. № 484-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 48. – Ст. 6726.

67. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации»: в ред. Федерального закона от 24 апреля 2020 г. № 147-ФЗ // Собрание законодательства Российской Федерации. – 2011. – № 48. – Ст. 6724.

68. Федеральный закон от 28 декабря 2013 г. №442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации»: в ред. Федерального закона от 1 мая 2019 г. № 91-ФЗ // Собрание законодательства Российской Федерации. – 2013. – № 52. – Ст. 7007.

69. Федеральный закон от 29 ноября 2007 г. № 282-ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»: в ред. Федерального закона от 18 апреля 2018 г. № 74-ФЗ // Собрание законодательства Российской Федерации. – 2007. – № 49. – Ст. 6043.

70. Федеральный закон от 08 июля 1999 г. №183-ФЗ «Об экспортном контроле»: в ред. Федерального закона от 13 июля 2015 г. № 216-ФЗ) // Собрание законодательства Российской Федерации от 26.07.1999 – № 30 – Ст. 3774.

71. Федеральный закон от 29 ноября 2009 г. № 261-ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации»: в ред. Федерального закона от 26 июля 2019 г. № 241-ФЗ // Собрание законодательства Российской Федерации. – 2009. – № 48. – Ст. 5711.

72. Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-1: в ред. Федерального закона о 27 декабря 2019 г. № 480-ФЗ // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. – 1993. – № 10. – Ст. 357.

73. Указ Президента Российской Федерации от 30 ноября 1995 г. №1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне»: Указ Президента РФ от 30.11.1995 № 1203 // Собрание законодательства Российской Федерации. – 1995. – № 49. – Ст. 4775.

74. Постановление Правительства Российской Федерации от 31 июля 2014 г. № 758 «О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей»: // Собрание законодательства Российской Федерации. – 2014. – № 32 – Ст. 4525.

75. Постановление Правительства Российской Федерации от 27 августа 2005 г. № 538 «Об утверждении Правил взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность» // Собрание законодательства Российской Федерации. – 2005. – № 36. – Ст. 3704.

76. Приказ Генпрокуратуры Российской Федерации, МВД России, МЧС России, Минюста России, ФСБ России, Минэкономразвития России, ФСКН России от 29.12.2005 г. № 39/1070/1021/253/780/353/399 «О едином учете преступлений» // Российская газета – 2006. – № 13.

Материалы судебной практики

77. Архив Ленинского районного суда г. Тюмени, 2000 г., уголовное дело № 1-2549/2000.

78. Архив ГУВД Свердловской области, 1998 г., уголовное дело № 176709, возбужденное 10.03.1998 г. по ст. 273 ч. 1 УК РФ.

79. Архив Кстовского городского суда Нижегородской области, 2002 г., уголовное дело № 1-148/2002.

80. Архив Октябрьского районного суда г. Кирова, 2002 г., уголовное дело № 1-160/2002.

81. Архив Новгородского городского суда Новгородской области, 2001 г., уголовное дело № 1-3/2001.

82. Архив Октябрьского районного суда г. Улан-Удэ, 2001 г., уголовное дело № 1-4488/2001.

83. Архив Ангарского городского суда Иркутской области, 2003 г., уголовное дело № 1-343/2003.

84. Архив Свердловского районного суда г. Иркутска, 2000 г., уголовное дело № 1-700/2000.

85. Архив Кавказского районного суда Краснодарского края, 2001 г., уголовное дело № 1-241/2001.

86. Архив Касимовского городского суда Рязанской области, 1999 г., уголовное дело № 1-170/1999.

87. Архив Петропавловск-Камчатского городского суда Камчатской области, 2002 г., уголовное дело № 1-178/2002.

88. Архив Городецкого районного суда Нижегородской области, 2003 г., уголовное дело № 1-171/2003.

89. Архив Свердловского районного суда г. Белгорода, 2012 г., уголовное дело № 1-73/2012.

90. Архив Шебалинского районного суда Республики Алтай, 2013 г., уголовное дело № 1-6/2013.

91. Архив Саянского городского суда Иркутской области, 2014 г., уголовное дело № 1-14/2014.

92. Архив Рузского районного суда Московской области, 2015 г., уголовное дело № 1-49/2015.

93. Архив Автозаводского районного суда г. Тольятти, 2016 г., уголовное дело № 1-834/2016.

94. Архив Кировского районного суда г. Омска, 2016 г., уголовное дело № 1-363/2016.

95. Архив Свердловского районного суда г. Перми, 2015 г., уголовное дело № 1-8/2015.

96. Архив Октябрьского районного суда г. Иркутска, 2016 г., уголовное дело № 1-50/2016.

97.

98. Архив Кировского районного суда г. Иркутска, 2017 г., уголовное дело № 1-182/17.

99. Архив Новочеркасского городского суда Ростовской области, 2018 г., уголовное дело № 1-351/2018.

100. Архив Кировского районного суда г. Иркутска, 2018 г., уголовное дело № 1-264/2018.

101. Архив Кировского районного суда г. Иркутска, 2020 г., уголовное дело № 1-53/2020.

Научная и учебная литература

99. *Батурин, Ю. М.* Проблемы компьютерного права / Ю. М. Батурин. – М.: Юрид. лит., 1991. – 272 с.

100. *Белкин, А.Р.* Теория доказывания в уголовном судопроизводстве. – М.: Изд-во Норма, 2005. – 415 с.

99. *Вехов, В.Б.* Компьютерные преступления: Способы совершения. Методики расследования. М.: Право и Закон, 1996. – 182 с.

100. *Вехов, В.Б., Голубев, В.А.* Расследование компьютерных преступлений в странах СНГ: Монография / В.Б. Вехов, В.А. Голубев // под ред. Б.П. Смагоринского. – Волгоград: ВА МВД России, 2004. – 304 с.

101. Воронин Ю А. Введение в криминологию: курс лекций. М., 2008. 103 с.

101. *Гаврилов В.М.* Противодействие преступлениям, совершаемым в сфере компьютерной и мобильной коммуникации организованными преступными

группами. Саратов: Саратовский Центр по исследованию проблем организованной преступности и коррупции: Сателлит, – 2009. – 191 с.

102. *Гаухман, Л. Д., Колодкин, Л.М., Максимов, С. В.* Уголовное право: Часть Общая. Часть Особенная: учебник. 2-е изд., перераб и доп. М., – 1999. – 652 с.

103. Гилинский Я.И. Девиантология. СПб.: Юрид. центр Пресс, 2004. – 455 с.

104. *Гиляревский, Р.С.* Информатика как наука об информации: информационный, документальный, технологический, экономический, социальный и организационный аспекты / Р.С. Гиляревский. – М.: Фаир-Пресс, 2006 – 466 с.

102. *Дремлюга, Р.И.* Интернет-преступность Монография / Дремлюга Р.И.; Ред.: Дроздов В.Г. – Владивосток: Изд-во Дальневост. ун-та, 2008. – 238 с.

103. *Ковалева, Н.Н.* Информационное право России // Учебное пособие. – М., 2007. – 362 с.

105. *Кузнецов, М. В.* Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. – СПб.: БХВ-Петербург, 2007. – 368 с.

104. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. – М, – 2013. – 25 с.

105. *Новиков, С.Н.* Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи / под ред. В.П. Шувалова. М.: ООО «Горячая линия-Телеком», – 2015. – с. 128.

106. *Осипенко, А.Л.* Сетевая компьютерная преступность: теория и практика борьбы: Монография / Осипенко А.Л. – Омск: Изд-во Омск. акад. МВД России, – 2009. – 480 с.

106. *Полевой, Н.С.* Криминалистическая кибернетика. – М.: Изд-во МГУ, – 1982. – 113 с.

107. *Рарог,* А.И. Качество уголовного закона: проблемы Особенной части: монография / отв. ред. А. И. Рарог. М.: Проспект, 2017. – с. 295.

108. *Репецкая А.Л., Рыбальская В.Я*. Криминология: Часть Общая: учебное пособие. – Иркутск, – 1999. – 240 с.

109. *Репецкая, А.Л.* Транснациональная организованная преступность // Учебное пособие. – Иркутск: Издательство БГУЭП, 2005. – 91 с.

110. *Савельева, В.С.* Основы квалификации преступлений: учебное пособие. – 2013. – 60 с.

111. *Сапранкова, Т.Ю.* Проблемы систематизации преступлений, связанных с нарушением неприкосновенности частной жизни // Успехи современной науки. – 2017. – № 3. – 245 с.

112. *Сачков, Д.И., Смирнова, И.Г.* Обеспечение информационной безопасности в органах власти: учебное пособие // Д.И. Сачков, И.Г. Смирнова / Иркутск: Изд-во: БГУЭП, 2015. – 121 с.

113. *Смирнова, И.Г.* Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / под науч. ред. И. Г. Смирновой. М.: Юрлитинформ, – 2016. – 312 с.

114. *Степанов-Егиянц, В.Г.* Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации. – М.: Статут, 2016. – 190 с.

115. *Шувалов, В.П.* Методология защиты пользовательской информации на основе технологий сетевого уровня мультисервисных сетей связи. – М.: ООО «Горячая линия-Телеком», 2015. 128 с.

Научные статьи в журналах и периодических изданиях

107. *Акиндеева, А.В.* Кардинг в сфере оборота банковских карт // А.В. Акиндеева / Ученые записки Санкт-Петербургского им. В.Б. Бобкова филиала Российской таможенной академии. – 2005. – № 2 (24). – С. 263-271

108. *Александров, А.С., Кувычков, С.И.* О надежности электронных доказательств в уголовном процессе // Библиотека криминалиста. – 2013. – № 5 – С. 76-84.

109. *Батоев, В.Б., Семенчук, В.В*. Использование криптовалюты в преступной деятельности: проблемы противодействия // Труды Академии управления МВД России. – 2017. – № 2 (42). – С. 9–15

110. *Бегишев, И.Р.* Преступления в сфере обращения цифровой информации // Информационное право. – 2010. – № 2. – С. 18-21.

111. *Богданова, Т.Н.* К вопросу об определении понятия «Преступления в сфере компьютерной информации» // Вестник Челябинского государственного университета. – 2012. – № 37 (291). – С. 64-67.

112. *Борздыко, И.А., Черномазов, Н.М.* Применение FTP серверов для обмена и хранения пользовательской информации // Современные научные исследования и инновации. – 2016. – №1. – С.233-234.

113. *Быков, В.М., Черкасов, В.Н.* Новый закон о преступлениях в сфере компьютерной информации: ст.272 УК РФ // Российский судья. – 2012. –№5. – С. 14-19.

114. *Быков, В.М., Черкасов, В.Н.* Новая редакция ст. 274 УК // Законность. – 2012. – М. – № 2. – С. 25-29.

115. *Вальвачев, В.В.* Динамика цифрового неравенства в современном мире // Научные проблемы гуманитарных исследований. – 2010. – №7. – С. 270-279.

116. *Васюков, В.Ф.* Отдельные вопросы производства осмотра при расследовании преступлений, совершаемых с использованием криптовалюты // Современное уголовнопроцессуальное право России - уроки истории и проблемы дальнейшего реформирования: Сб. мат-лов Междун. науч-практ. конф. К 300-летию российской полиции и 100-летию советской милиции. Орловский юридический институт МВД России имени В. В. Лукьянова. – 2017. – С. 83-87.

117. *Вехов, В.Б.* Работа с электронными доказательствами в условиях изменившегося уголовно-процессуального законодательства // Российский следователь. – 2013. – № 10. – С. 22

118. *Воронцова,* С.В. Киберпреступность: проблемы квалификации преступных деяний. Российская юстиция. – 2011. – №2. – С. 14-15.

119. *Галушин*, П.В., *Карлов*, *А.Л.* Сведения об операциях с криптовалютами (на примере биткойна) как доказательство по уголовному делу // Ученые записки Казанского юридического института МВД России. 2017. Т. 2. № 4. С. 90-100.

120. *Герасимова, О.А.* Особенности преступлений в сфере компьютерной информации // Вестник ТГУ, 2007. – № 12 (56). – С. 327–330.

121. *Горбунов, А.Н., Цимбал, В.Н.* Способы незаконного использования пластиковых карт при совершении преступлений // А.Н. Горбунов, В.Н. Цимбал / Общество и право. – № 3 (45). – 2013. – С. 217-221

122. *Дворецкий, М.Ю.* Уголовная ответственность за мошенничество в сфере компьютерной информации: проблемы теории и правоприменительной практики // Вестник ТГУ. – 2013. – № 8 (124). – С. 407-410.

123. *Дельцова, Т.А*. Денежные суррогаты в российской федерации: прошлое, настоящее, будущее // Вестник Калининградского филиала Санкт-Петербургского университета МВД России. – 2016. – № 1 (43). – С. 164-166.

124. *Евдокимов, К.Н.* Вопросы уголовно-правовой квалификации неправомерного доступа к компьютерной информации и его отграничения от смежных составов преступлений // Вестник Академии Генеральной прокуратуры РФ, 2009. – № 10. – С. 42–46.

125. *Ефремов, К.А.* Личность преступника, совершающего преступления в сфере компьютерной информации // Общество: политика, экономика, право. – 2016. - № 6. – С. 92-95.

126. *Жиделев, В.Г.* Некоторые аспекты квалификации преступлений в сфере компьютерной информации в российском и зарубежном законодательстве // Человек: преступление и наказание. – 2012. – № 2. – С. 23-25.

127. *Жилина, И.Ю*. Киберпреступность и борьба с ней (сводный реферат) // Социальные и гуманитарные науки. Отечественная и зарубежная литература. Сер. 2, Экономика: реф. журн. – 2003. – № 1. – С. 144–148.

128. *Жмуров, Д.В.* Даркнет как ускользающая сфера правового регулирования // Сибирские уголовно-процессуальные и криминалистические чтения. – 2020. –№ 1.– С. 89-98.

129. *Иванов, Н.А.* Криминалистические классификации цифровой информации // Вестник Омской юридической академии. – 2013. – № 1 (20). – С. 81-84.

130. *Иванов, Н.А.* Цифровая информация в уголовном процессе // Библиотека криминалиста. – 2013. – №5 (10). – С. 93-102.

131. *Ищенко, Е.П.* Киберпреступность: криминалистический аспект проблемы //Библиотека криминалиста. -2013. - № 5. - С. 181–192.

132. *Карпова, Д.Н.* Киберпреступность: глобальная проблема и ее решение / Д.Н. Карпова // Власть. — 2014. — № 8. — С. 46–50.

133. *Коломинов, В.В.* О способе совершения мошенничества в сфере компьютерной информации // Человек: преступление и наказание. – 2015. № 3. – С. 145–149.

134. *Лысак, Е.А.* Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ – № 90. – 2013. – С. 997-1006.

135. *Мерзлов, Ю.А*. Криминологический портрет лиц, совершающих преступления в сфере компьютерной информации // Правопорядок: история, теория, практика. – 2015. – №4 (7). – С. 56-61.

136. *Морар, И.О.* Как выглядит социально-правовой портрет участника преступного формирования, совершающего компьютерные преступления /И. О. Морар // Российский следователь. – 2012. – №13. – С. 34–37.

137. *Морар, И.О.* Могут ли в рамках науки криминологии рассматриваться способы совершения компьютерных преступлений и их последствия? // Российский следователь – Юрист М. – № 12. – С. 37–41.

138. *Номоконов, В.А., Тропина, Т.Л.* Киберпреступность: прогнозы и проблемы борьбы // В.А. Номоконов, Т.Л. Тропина / Библиотека криминалиста. – № 5 (10). – 2013. – С. 148 -160.

139. *Овсюков, Д.А.* Блокирование информации в информационно-телекоммуникационной сети Интернет путем создания искусственной перегрузки компьютерной системы: уголовно-правовой анализ // Российский следователь. – 2014. – № 4. – С. 35-39.

140. *Октябрева, М.С.* Кардинг в российской практике // М.С. Октябрева / Экономика и управление: анализ тенденций и перспектив развития – № 15. – 2014. – С. 99-103

141. *Осипенко, А.Л.* Проблемы вовлечения электронно-цифровых следов в уголовный процесс // Научный вестник Омской академии МВД России. – 2009. – № 4 (35). – С. 31-34.

142. *Остапенко, Г.А., Бурса, М.В., Иванкин, Е.Ф.* Аналитическое моделирование процесса реализации Ddos-атаки типа HTTP-flood. // Информационная безопасность. –2013. – № 1. – С. 107–110.

143. *Павленко, И.А., Смагоринский, Б.П.* О современном состоянии расследования хищений денежных средств с использованием банковских карт на территории Российской Федерации // Б.П. Смагоринский, И.А. Павленко / Вестник Волгоградской академии МВД России. – № 1 (20). – 2012. – С. 166-172.

144. *Попов, А.Б.* Проблемы квалификации преступлений в сфере компьютерной информации // Вестник ТГУ, 2008. – № 10 (66). – С. 339–344.

145. *Простосердов, М.А.* Криптовалюта как предмет хищения // Российское правосудие. – 2016. – № 6 (122). – С. 107-111.

146. *Протасевич, А.А., Зверянская, Л.П.* Способы совершения преступлений с использованием поддельных банковских карт // Актуальные

проблемы теории и практики правотворчества и правоприменения (к 20-летию юридического образования в БГУЭП): сб. науч. тр. / редколлегия В.Н. Андриянов, А.А. Протасевич, Ю.В. Арбатская. Иркутск, 2015. – С. 127-132.

147. Репецкая А.Л., Родивилин И.П. Незаконное ограничение доступа к компьютерной информации в сети Интернет: уголовно правовой аспект // Библиотека уголовного права и криминологии. – 2016. – № 3(15). – С. 79-84.

148. *Рогозин, В.Ю.* Изменения в криминалистических характеристиках преступников в сфере высоких технологий // Расследование преступлений: проблемы и пути их решения. – 2015. № 1 (7). – С. 56–58.

149. *Родивилин И.П.* Особенности характеристики состояния и структуры преступлений в сфере обращения охраняемой законом информации в современный период Российской Федерации // Вестник Восточно-Сибирского института МВД России. – 2020. – № 1. – С. 64-72.

150. *Родивилин И.П.* Современная специфика детерминации преступлений в сфере обращения охраняемой законом информации // Вестник УДГУ. – 2021. – № 2. – С. 305-311.

151. *Родивилин И.П.* Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния // Научный вестник Омской академии МВД России. – 2017. – № 4 (67). – С. 25-29.

152. *Родивилин И.П.* Уголовно-правовое и криминологическое противодействие вэб-кардингу // Библиотека уголовного права и криминологии. – 2017. – № 1(19). – С. 128.

153. *Родивилин И.П.* Цифровое неравенство – угроза безопасности Российской Федерации // Материалы Международной научно-практической конференции «Проблемы обеспечения национальной безопасности в контексте изменения геополитической ситуации». – 2017. – С. 139-143.

154. *Родивилин И.П., Коломинов В.В., Брыжак Д.Э.* Интеллектуальный разврат несовершеннолетних в сети Интернет // Сибирские уголовно-процессуальные и криминалистические чтения. – 2020. – № 1. – С. 64-76.

155. *Родивилин И.П., Родивилина В.А.* Защита цифровых прав человека // Материалы Всероссийской научно-практической конференции «Конституция Российской Федерации и правовая политика на современном этапе». –2019. – С. 104-110.

156. *Родивилин И.П., Родивилина В.А.* Информационное оружие // Материалы Международного Байкальского форума Евразийский интеграционный проект: цивилизационная идентичность и глобальное позиционирование». – 2018. – С. 276.

157. *Родивилин И.П., Родивилина В.А.* Криптовалюта как объект преступления // сборник материалов международной научно-практической конференции «Деятельность правоохранительных органов современных условиях». – 2018. – С. 262-265.

158. Сидоренко Э.Л. Криптовалюта как новый юридический феномен // Общество и право. – 2016. – №3 (57). – С. 193-197.

159. *Симаков, А.А.* Анонимность в глобальных сетях // Научный вестник Омской академии МВД России. – 2017. – № 2 (65). – С. 62-65.

160. *Сорокин, О.Л., Сидоркина, И.Г.* Анализ представления пользовательской информации в приборе «ТЕРЕМ-4» для измерения температуры ограждающих конструкций // Кибернетика и программирование. – 2015. – №5. – С. 193–198.

161. *Степанов-Егиянц, В.Г.* Объективная сторона неправомерного доступа к компьютерной информации по уголовному кодексу РФ // Библиотека криминалиста. – 2013. – № 5 (10). – С. 42-47.

162. *Титарева, Е.Г.* Мошенничество, совершаемое с использованием информационно-телекоммуникационных технологий // Научный альманах. – 2015. – № 7. – С. 1158-1161.

163. *Ткачев, А.В.* Использование электронных (компьютерных) документов в качестве документов-доказательств и письменных доказательств в

процессуальных отношениях // Библиотека криминалиста. – 2013. – № 5 (10). – С. 128-130.

164. *Унучек, Р.С.* Чебышев Мобильные угрозы // Вопросы кибербезопасности. – 2014. – № 3(4). – С. 57-59.

165. *Филимонов, С.А.* Ошибки и затруднения, возникающие при квалификации киберпреступлений// Библиотека криминалиста. – 2013. – №5(10). – С. 48-54.

166. Халиулилн А.И. Неправомерное копирование как последствие преступления в сфере компьютерной информации // Российский следователь. – 2015.– № 8. – С. 25.

167. *Чекунов, И.Г.* Криминологические и уголовно-правовые аспекты предупреждения киберпреступлений. – Российский следователь. – №3. – 2013. – С.36–43.

168. *Чирков, П.А.* Об объекте преступлений в сфере компьютерной информации в российском уголовном праве // Правовые вопросы связи. – 2012 – № 1. – С. 21-23.

169. *Шахрай, С.С.* К вопросу о способах совершения преступлений в сфере компьютерной информации // Вестник экономической безопасности. – 2009. № 10. – С. 98–102.

Диссертации и авторефераты диссертаций

176. *Вехов, В.Б.* Криминалистическое учение о компьютерной информации и средствах ее обработки: дис. ... д-ра юрид. наук. – Волгоград: ВА МВД России, 2008. – 561 с.

177. *Гаджиев, М.С.* Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан): дис. ... канд. юрид. наук: 12.00.08. Махачкала, 2004. – 168.

178. *Гайфутдинов, Р.Р.* Понятие и квалификация преступлений против безопасности компьютерной информации: дисс…. канд. юрид. наук. Казань. 2017. – 243 с.

179. *Гутник, С.И.* Уголовно-правовая характеристика преступных посягательств в отношении персональных данных: автореферат дисс… канд. юрид. наук. – Владивосток., 2017. – 24 с..

180. *Ефремова, М.А.* Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук.– М., – 2017. – 427 с.

181. *Зигура, Н.В.* Компьютерная информация как вид доказательств в уголовном процессе России дисс…. канд. юрид. наук. – Челябинск, 2010. – 234 с.

182. *Зубова, М.А.* Компьютерная информация как объект уголовно-правовой охраны: дисс…. канд. юрид. наук. – Казань., 2008. – 215 с.

183. *Карпов, В.С.* Уголовная ответственность за преступления в сфере компьютерной информации: дис. … канд. юрид. наук: 12.00.08 / В. С. Карпов. – Красноярск, 2002. – 202 с.

184. *Лопатина, Т.М.* Криминологические и уголовно-правовые основы противодействия компьютерной преступности: дисс…. докт. юрид. наук. – М., 2007. – 418 с.

185. *Малыковцев, М.М.* Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дисс…. канд. юрид. наук. – М, 2007. – 186 с.

186. *Маслакова, Е.А.* Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дисс…. канд. юрид. наук. – Орел. 2008. – 198 с.

187. *Мещеряков, В.А.* Основы методики расследования преступлений в сфере компьютерной информации: дис. … д-ра юрид. наук. – Воронеж, 2001. – 386 с.

188. *Простосердов, М.А.* Экономические преступления, совершаемые к киберпространстве, и меры противодействия им: дисс…. канд. юрид. наук. М., – 2016. – 232 с.

189. *Рудых, А.А.* Информационно-технологическое обеспечение криминалистической деятельности по расследованию преступлений в сфере информационных технологий: дис. ... канд. юрид. наук. Ростов-на-Дону, – 2020. – 239 с.

190. *Сало, И.А.* Преступные действия с компьютерной информацией ограниченного доступа: автореферат дисс… канд. юрид. наук. – М., 2011. – 285 с.

191. *Сафронов, О.М.* Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования: дисс…. канд. юрид. наук. –М., 2015. – 218 с.

192. *Спирина, С.Г.* Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: дис. … канд. юрид. наук. – Краснодар, 2001. – 242 с.

193. *Старичков, М.В.* Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дисс…. канд. юрид. наук. – Иркутск., 2006. – 237 с.

194. *Суслопаров, А.В.* Компьютерные преступления как разновидность преступлений информационного характера: дисс…. канд. юрид. наук. – Красноярск, 2010. – 206 с.

195. *Тропина, Т.Л.* Киберпреступность: понятие состояние, уголовно-правовые меры борьбы дисс…. канд. юрид. наук. – Владивосток. 2005. – 234 с.

196. *Туликов,* А.В. Информационная безопасность и права человека в условиях постиндустриального развитая (теоретико-правовой анализ): дис. ... канд. юрид. наук. – М., – 2017. – 180 с.

197. *Хурум, М.А.* Преступления, связанные с получением и (или) разглашением конфиденциальной информации: криминализация, систематизация

и оптимизация законодательного описания: дис. … канд. юрид. наук. Краснодар., – 2019. – 220 с.

198. *Шахрай, С.С.* Система преступлений в сфере компьютерной информации: автореф. дис. … канд. юрид. наук. М., – 2010. – 28 с.

199. *Шахрай, С.С.* Система преступлений в сфере компьютерной информации: сравнительно-правовой, социолого-криминологический и уголовно-правовой аспекты: дисс…. канд. юрид. наук. М, – 2010. – 161 с.

200. *Щепетильников, В.Н.* Уголовно-правовая охрана электронной информации: автореф. дис. … канд. юрид. наук. Елец, – 2006. – 179 с.

Электронные ресурсы

201. «State of the internet» – Режим доступа: https://www.akamai.com/us/en/multimedia/documents/report/q3-2015-soti-connectivity-final.pdf.

202. «Цифровая личность» за копейки – Режим доступа: https://www.comnews.ru/content/115730/2018-11-12/cifrovaya-lichnost-za-kopeyki.

203. INFOWATCH: Глобальное исследование утечек конфиденциальной информации в 2016 году – Режим доступа: https://www.infowatch.ru/report2016.

204. TOP 20 COUNTRIES WITH THE HIGHEST NUMBER OF INTERNET USERS – Режим доступа: http://www.internetworldstats.com/top20.htm.

205. Worst Passwords of 2018 – Режим доступа: https://www.teamsid.com/splashdatas-top-100-worst-passwords-of-2018.

206. Аккулы С.Х. В интернет-клуб можно теперь зайти только с паспортом // Радио Азаттык – Режим доступа: http://rus.azattyq.org/a/internet_cafe_restictions_kazakhstan/24478911.html.

207. Аудитория интернета в России в 2020 году – Режим доступа: https://mediascope.net/news/1250827.

208. Большой Энциклопедический словарь – Режим доступа: http://dic.academic.ru/dic.nsf/enc3p/200774.

209. Борис Мирошников: Сетевой фактор. Интернет. – Режим доступа: labirint.ru/books/494759.

210. Васильев В. А. Проблемы развития законодательства в сфере борьбы с киберпреступностью – Режим доступа: http://crime-research.ru/articles/vasil06.

211. Виртуальные валюты. Ключевые определения и потенциальные риски в сфере ПОД/ФТ: отчет ФАТФ. – Режим доступа: http://www.eurasiangroup.org/files/FATF_docs/Virtualnye_valyuty_FATF_2014.pd.

212. Глобальное исследование утечек конфиденциальной информации в I полугодии 2016 года – Режим доступа: https://www.infowatch.ru/sites/default/files/report/analytics/russ/InfoWatch_Global_Report_2016_ half_year.pdf?rel=1.

213. *Добрынин, Ю.В.,* Классификация преступлений в сфере компьютерной информации // Право и Интернет – Режим доступа: http://www.russianlaw.net/law/computer_crime/a158.

214. Законопроект № 1112019-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с введением понятия уголовного проступка» – Режим доступа: https://sozd.duma.gov.ru/bill/1112019-7.

215. Заседание коллегии МВД России – Режим доступа: http://kremlin.ru/events/president/news/62860.

216. Зачем в социальных сетях система распознавания лиц [электронный ресурс] // gazeta.ru. URL: https://www.gazeta.ru/tech/2018/03/10/11675389/face_recognition.shtml.

217. Интернет в России: динамика проникновения. Лето 2017 г. // fom.ru Фонд Общественное Мнение. – Режим доступа: http://fom.ru/SMI-i-internet/13783.

218. Интернет в цифрах и фактах – Режим доступа: http://compress.ru/article.aspx?id=14772.

219. Интернет: новая эра мобильных устройств // Всероссийский центр изучения общественного мнения (ВЦИОМ) – Режим доступа: http://wciom.ru/index.php?id=236&uid= 115255.

220. Итальянские интернет-кафе начали ксерокопировать паспорта клиентов – Режим доступа: https://lenta.ru/news/2005/10/05/cafe.

221. Киберпреступность в цифрах – Режим доступа: https://www.aktiv-company.ru/analitics/articles/cybercryme.html.

222. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2020 года – Режим доступа: https://xn--b1aew.xn--p1ai/reports/item/22678184.

223. *Лацинская, М.* Group-IB представила отчет о хакерских атаках // Газета.Ру. 2016 г. 13 окт. – Режим доступа: https://www.gazeta.ru/tech/2016/10/13/10249697/cybercrimecon_2016.shtml.

224. *Майоров, А.В.* Понятие и структура системы противодействия преступности // Правопорядок: история, теория, практика. 2014. №1 (2) – Режим доступа: http://cyberleninka.ru/article/n/ponyatie-i-struktura-sistemy-protivodeystviya-prestupnosti.

225. *Манойло, А.В.* Объекты и субъекты информационного противоборства. – Режим доступа: http://psy.piter.com/Hbrary/?tp=1&rd=8&l=636&p=1293.

226. Оксфордский словарь английского языка (Oxford English Dictionary) – Режим доступа: http://www.oed.com/view/Entry/37975/

227. Оценка объемов рынка киберпреступности в РФ – Режим доступа: http://report2013.group-ib.ru.

228. РКН потребовал заблокировать телеграм-боты по «пробиву данных» граждан – Режим доступа: https://www.interfax.ru/russia/755038.

229. Словарь иностранных слов русского языка – Режим доступа: http://dic.academic.ru/dic.nsf/dic_fwords/21984

230. Современный толковый словарь русского языка Ефремовой – Режим доступа: http://dic.academic.ru/dic.nsf/efremova/177218.

231. Стратегия развития информационного общества в Российской Федерации на 2017 – 2030 годы (проект) – Режим доступа: http://www.scrf.gov.ru/documents/6/136.html.

232. *Сулейманов С.* Deepfakes: порно, в которое нейросеть добавляет лица знаменитостей. Его запрещают все крупные сервисы, даже PornHub // Медуза. 2018 // URL: https://meduza.io/feature/2018/02/07/deepfakes-porno-v-kotoroe-neyroset-dobavlyaet-litsa-znamenitostey-ego-zapreschayut-vse-krupnye-servisy-dazhe-pornhub.

233. Толковый словарь Ожегова – Режим доступа: http://dic.academic.ru/dic.nsf/ogegova/108750.

234. Толковый словарь Ожегова – Режим доступа: http://dic.academic.ru/dic.nsf/ogegova/88986.

235. Толковый словарь Ушакова – Режим доступа: http://dic.academic.ru/dic.nsf/ushakov/840342.

236. *Фатьянов, А.А.* Правовой анализ категории «электронные денежные средства» в российском законодательстве. Гражданское общество в России и за рубежом. 2014.№ 3. // СПС «КонсультантПлюс».

237. *Хазов, В.* Все, что вам надо знать о разнице между IPv4 и IPv6 – Режим доступа: http://blog.vasexperts.ru/?p=815.

238. Что такое Фишинг – Режим доступа: https://support.kaspersky.ru/viruses/general/2313.

Иностранные источники

239. *Huey, L.* Uppity civilians and cyber-vigilantes: The role of the general public in policing cyber-crime / L. Huey, J. Nhan, R. Broll // Criminology and Criminal Justice. – 2013. – Vol. 13, № 1. – P. 81–97. – DOI : 10.1177/1748895812448086.

240. *Shah, S.A.* Biological and Psychophysiological Factors in Criminality / S.A. Shah, H.R. Loren. Handbook of Criminology. Chicago: Rand McNally, 1974.-Pp. 101-173.

241. *Smith, R.G.* Criminals on Trial / R.G. Smith, P. Grabosky, G. Urbas. – Cambridge University Press, 2004. – 263 p.

242. *Surgeon, B.* Хакеры // Компьютерра. – 1996. - № 43. – С. 22.

243. *Айков, Д.* Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями / Д. Айков, К. Сейгер, У. Фонсторх; Пер. с англ. В.И. Воропаева, Г.Г. Трехалина. – М.: Мир, 1999. – 351 с.

244. *Бояркина, Л.А., Бояркин, В.В.* Цифровой след и цифровая тень как производные персональных данных // Сборники конференций НИЦ Социосфера. – Прага: Vedecko vydavatelske cen-trum Sociosfera-CZ s.r.o., – 2016. – № 62. – С. 71–78.

ПРИЛОЖЕНИЯ

Приложение 1.

Классификация информации по виду нормативно-правового акта, относящего информацию к сведениям ограниченного доступа.

1. Государственная тайна – режим ограниченного доступа устанавливается ст. 5 Закона Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»[1], Указом Президента РФ «Об утверждении Перечня сведений, отнесенных к государственной тайне»[2].

2. Коммерческая тайна – ФЗ «О коммерческой тайне»[3], ст. 12 ФЗ «Об инвестиционном товариществе»[4].

3. Конфиденциальность персональных данных (любой информации, относящейся прямо или косвенно к определенному или определяемому физическому лицу (субъекту персональных данных)) – ст. 7 ФЗ «О персональных данных»[5].

4. Налоговая тайна – ст. ст. 102 и 313 Налогового кодекса РФ[6].

5. Банковская тайна – ст. 857 Гражданского кодекса РФ (часть вторая)[7],

---

[1] О государственной тайне: Закон РФ от 21.07.1993 № 5485-1 (в ред. ФЗ от 08.03.2015 г. №23-ФЗ) // Собрание законодательства Российской Федерации. 1997. №41. Ст. 4673.

[2] Об утверждении Перечня сведений, отнесенных к государственной тайне: Указ Президента РФ от 30.11.1995 № 1203 // Собрание законодательства РФ. 1995. № 49. Ст. 4775.

[3] О коммерческой тайне: Федеральный закон от 29.07.2004 № 98-ФЗ (в ред. ФЗ от 12.03.2014 г. № 35-ФЗ) // Собрание законодательства РФ. 2004. №32. Ст. 3283.

[4] Об инвестиционном товариществе: Федеральный закон от 28.11.2011 № 335-ФЗ (в ред. ФЗ 21.07.2014 г. № 220-ФЗ) // Собрание законодательства РФ. 2011. №49. Ст. 7013.

[5] Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»: в ред. Федерального закона от 27 декабря 2019 г. № 480-ФЗ // Собрание законодательства Российской Федерации. – 2006. – № 31. – Ст. 3451.

[6] Налоговый кодекс Российской Федерации (часть 1): Федеральный закон от 31.07.1998 № 146-ФЗ (в ред. ФЗ от 13.07.2015 г. № 232-ФЗ) // Собрание законодательства РФ. 1998. № 31. Ст. 3824; Налоговый кодекс Российской Федерации (часть 2): Федеральный закон от 05.08.2000 № 117-ФЗ (в ред. ФЗ от 13.07.2015 г. № 232-ФЗ) // Собрание законодательства РФ. 2000. № 32. Ст. 3340.

[7] Гражданский кодекс РФ (часть вторая): Федеральный закон от 26.01.1996 № 14-ФЗ (в ред. ФЗ от 13.07.2015 г. № 268-ФЗ) // Собрание законодательства РФ. 1996. №5. Ст. 410.

ст. 26 ФЗ «О банках и банковской деятельности»[1], ст. 57 ФЗ «О Центральном банке Российской Федерации (Банке России)»[2].

6. Врачебная тайна – ст. ст. 13, 92 ФЗ «Об основах охраны здоровья граждан в Российской Федерации»[3], ст. 15 Семейного кодекса РФ[4], ст. 9 Закона РФ «О психиатрической помощи и гарантиях прав граждан при ее оказании»[5], ст. 14 Закона РФ «О трансплантации органов и (или) тканей человека»[6], ст. 13 ФЗ «О донорстве крови и ее компонентов»[7].

7. Нотариальная тайна – ст. 16 и 28 Основ законодательства Российской Федерации о нотариате[8], ст. 26 Федерального закона от 05.07.2010 № 154-ФЗ «Консульский устав Российской Федерации»[9].

8. Адвокатская тайна – ст. 8 ФЗ «Об адвокатской деятельности и адвокатуре в Российской Федерации»[10].

---

[1] О банках и банковской деятельности: Федеральный закон от 02.12.1990 № 395-1 (в ред. ФЗ от 13.07.2015 г. № 259-ФЗ) // Собрание законодательства РФ. 1996. № 6. Ст. 492.

[2] О Центральном банке Российской Федерации (Банке России): Федеральный закон от 10.07.2002 № 86-ФЗ (в ред. ФЗ от 13.07.2015 г. № 231-ФЗ) // Собрание законодательства РФ. 2002. №28. Ст. 2790.

[3] Об основах охраны здоровья граждан в Российской Федерации: Федеральный закон от 21.11.2011 № 323-ФЗ (в ред. ФЗ от 13.07.2015 г. № 271-ФЗ) // Собрание законодательства РФ. 2011. №48. Ст. 6724.

[4] Семейный кодекс РФ: закон РФ от 29.12.1995 № 223-ФЗ (в ред. ФЗ от 13.07.2015 г. № 240-ФЗ) // Собрание законодательства РФ. 1996. №1. Ст. 6724.

[5] О психиатрической помощи и гарантиях прав граждан при ее оказании: Закон РФ от 02.07.1992 № 3185-1 (в ред. ФЗ от 08.03.2015 г. № 23-ФЗ) // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1992. №33. Ст. 1913.

[6] О трансплантации органов и (или) тканей человека: Закон РФ от 22.12.1992 № 4180-1 (в ред. ФЗ от 29.11.2007 г. № 279-ФЗ) // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1993. №2. Ст. 62.

[7] О донорстве крови и ее компонентов: Федеральный закон от 20.07.2012 № 125-ФЗ (в ред. ФЗ от 06.04.2015 г. № 68-ФЗ) // Собрание законодательства РФ. 2012. №30. Ст. 4176.

[8] Основы законодательства Российской Федерации о нотариате от 11.02.1993 № 4462-1 (в ред. ФЗ от 13.07.2015 г. № 259-ФЗ) // Ведомости Съезда народных депутатов РФ и Верховного Совета РФ. 1993. №10. Ст. 357.

[9] Консульский устав Российской Федерации: Федеральный закон от 05.07.2010 № 154-ФЗ (в ред. ФЗ от 21.07.2014 г. № 267-ФЗ) // Собрание законодательства РФ. 2010. №28. Ст. 3554.

[10] Об адвокатской деятельности и адвокатуре в Российской Федерации: Федеральный закон от 31.05.2002 №63-ФЗ (в ред. ФЗ от 13.07.2015 г. № 268-ФЗ) // Собрание законодательства РФ. 2002. №23. Ст. 2102.

9. Аудиторская тайна – ст. 9 ФЗ «Об аудиторской деятельности»[1], ст. 10 ФЗ «О содействии развитию жилищного строительства»[2].

10. Тайна страхования – ст. 946 Гражданского кодекса РФ (часть вторая), ст. 47 ФЗ «Об обязательном медицинском страховании в Российской Федерации»[3], ст. 32 ФЗ «О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования»[4], ст. 18 ФЗ «Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний»[5].

11. Тайна ломбарда – ст. 3 ФЗ «О ломбардах»[6].

12. Тайна связи – ст. 53 и 63 ФЗ «О связи»[7], ст. 15 ФЗ «О почтовой связи»[8].

13. Тайна завещания – ст. 1123 Гражданского кодекса РФ (часть третья)[9].

14. Тайна усыновления – ст. 139 Семейного кодекса РФ.

15. Тайна следствия – ст. 161 Уголовно-процессуального кодекса РФ[1], ст.

---

[1] Об аудиторской деятельности: Федеральный закон от 30.12.2008 № 307-ФЗ (в ред. ФЗ от 01.12.2014 г. №403-ФЗ) // Собрание законодательства РФ. 2009. №1. Ст. 15.

[2] О содействии развитию жилищного строительства: Федеральный закон от 24.07.2008 № 161-ФЗ (в ред. ФЗ от 13.07.2015 г. № 225-ФЗ) // Собрание законодательства РФ. 2008. №30 (часть II). – Ст. 3617.

[3] Об обязательном медицинском страховании в Российской Федерации: Федеральный закон от 29.11.2010 № 326-ФЗ (в ред. ФЗ от 01.12.2014 г. № 418-ФЗ) // Собрание законодательства РФ. 2010. №49. Ст. 6422.

[4] О страховых взносах в Пенсионный фонд Российской Федерации, Фонд социального страхования Российской Федерации, Федеральный фонд обязательного медицинского страхования: Федеральный закон от 24.07.2009 № 212-ФЗ (в ред. ФЗ от 13.07.2015 г. № 213-ФЗ) // Собрание законодательства РФ. 2009. №30. Ст. 3738.

[5] Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний: Федеральный закон от 24.07.1998 № 125-ФЗ (в ред. ФЗ от 01.12.2014 г. №406-ФЗ) // Собрание законодательства РФ. 1998. №31. Ст. 3803.

[6] О ломбардах: Федеральный закон от 19.07.2007 № 196-ФЗ (в ред. ФЗ 01.12.2014 г. № 406-ФЗ) // Собрание законодательства РФ. 1998. №31. Ст. 3803.

[7] О связи: Федеральный закон от 07.07.2003 № 126-ФЗ (в ред. ФЗ от 13.07.2015 г. № 263-ФЗ) // Собрание законодательства РФ. 2003. №28. Ст. 2895.

[8] О почтовой связи: Федеральный закон от 17.07.1999 № 176-ФЗ (в ред. ФЗ от 06.12.2011 г. № 409-ФЗ) // Собрание законодательства РФ. 1999. №29. Ст. 3697.

[9] Гражданский кодекс РФ (часть третья): Федеральный закон от 26.11.2001 № 147-ФЗ (в ред. ФЗ от 07.02.2017 г. № 12-ФЗ) // Собрание законодательства РФ. 2001. №49. Ст. 4552.

20 ФЗ «Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания»[2].

16. Тайна судопроизводства – ст. 194 Гражданского процессуального кодекса РФ[3], ст. 20 Арбитражного процессуального кодекса РФ[4], ст. 298 и 341 Уголовно-процессуального кодекса РФ.

17. Конфиденциальность отдельных сведений при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд – ст. ст. 51, 60, 66, 68 ФЗ «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд»[5].

18. Конфиденциальность сведений, ставших известными работнику органа записи актов гражданского состояния в связи с государственной регистрацией акта гражданского состояния – ст. 12 ФЗ «Об актах гражданского состояния»[6].

19. Конфиденциальность сведений о защищаемых лицах – ст. 9 ФЗ «О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства»[7], ст. 9 ФЗ «О государственной защите судей, должностных лиц

---

[1] Уголовно-процессуальный кодекс РФ: Федеральный закон 18.12.2001 № 174-ФЗ (в ред. ФЗ от 07.03.2017 г. № 33-ФЗ) // Собрание законодательства РФ. 2001. № 52 (часть I). Ст. 4921.

[2] Об общественном контроле за обеспечением прав человека в местах принудительного содержания и о содействии лицам, находящимся в местах принудительного содержания: Федеральный закон от 10.06.2008 № 76-ФЗ // Собрание законодательства РФ. 2011. №50. – Ст. 7353.

[3] Гражданский процессуальный кодекс РФ: Федеральный закон 14.11.2002 № 138-ФЗ (в ред. ФЗ от 19.12.2016 г. № 438-ФЗ) // Собрание законодательства РФ. 2002. №46. Ст. 4532.

[4] Арбитражный процессуальный кодекс РФ от 24.07.2002 № 95-ФЗ (ред. от 19.12.2016 № 435-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3012.

[5] О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: Федеральный закон от 05.04.2013 № 44-ФЗ (в ред. ФЗ от 07.06.2017 г. № 438-ФЗ) // Собрание законодательства РФ. 2013. №14. Ст. 1652.

[6] Об актах гражданского состояния: Федеральный закон от 15.11.1997 № 143 ФЗ (в ред. ФЗ от 03.07.2016 г. № 361-ФЗ) // Собрание законодательства РФ. 1997. № 47. Ст. 5340.

[7] О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства: Федеральный закон от 20.08.2004 № 119-ФЗ (в ред. ФЗ от 07.02.2017 г. № 7-ФЗ) // Собрание законодательства РФ. 2004. № 34. Ст. 3534.

правоохранительных и контролирующих органов»[1].

20. Конфиденциальность сведений, ставших известными гражданам в ходе оперативно-розыскной деятельности – ст. 17 ФЗ «Об оперативно-розыскной деятельности»[2].

21. Конфиденциальность сведений, содержащихся в личном деле и документах учета сотрудника органов внутренних дел, в реестре сотрудников органов внутренних дел, а также сведений о гражданах, поступающих на службу в органы внутренних дел – ст. ст. 39 и 40 ФЗ «О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации»[3].

22. Ограничение доступа к сведениям о доходах, об имуществе и обязательствах имущественного характера, представляемых государственными и муниципальными служащими, а также иными лицами, указанными в части 1 статьи 8 Федерального закона от 25.12.2008 № 273-ФЗ – ст. 8 ФЗ «О противодействии коррупции»[4], ст. 20 ФЗ «О государственной гражданской службе Российской Федерации»[5], ст. 15 ФЗ «О муниципальной службе в Российской Федерации»[6].

23. Ограничение доступа к сведениям о расходах по приобретению земельного участка, другого объекта недвижимости, транспортного средства,

---

[1] О государственной защите судей, должностных лиц правоохранительных и контролирующих органов: Федеральный закон от 20.04.1995 № 45-ФЗ (в ред. ФЗ от 07.02.2017 г. № 7-ФЗ) // Собрание законодательства РФ. 1995. № 17. Ст. 1455.

[2] Об оперативно-розыскной деятельности: Федеральный закон от 12.08.1995 №144-ФЗ (в ред. ФЗ от 06.06.2016 г. № 374-ФЗ) // Собрание законодательства РФ. 1995. № 33. Ст. 3349.

[3] О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 30.11.2011 № 342-ФЗ (в ред. ФЗ от 28.12.2016 г. № 505-ФЗ) // Собрание законодательства РФ. 2011. № 49 (ч. I). Ст. 7020.

[4] О противодействии коррупции: Федеральный закон от 25.12.2008 № 273-ФЗ (в ред. ФЗ от 28.12.2016 г. № 505-ФЗ) // Собрание законодательства РФ. 2008. № 52(ч. I). Ст. 6228.

[5] О государственной гражданской службе Российской Федерации: Федеральный закон от 27.07.2004 № 79-ФЗ (в ред. ФЗ от 28.12.2016 г. № 505-ФЗ) // Собрание законодательства РФ. 2004. № 31. Ст. 3215.

[6] О муниципальной службе в Российской Федерации: Федеральный закон от 02.03.2007 №25-ФЗ (в ред. ФЗ от 30.06.2016 г. № 224-ФЗ) // Собрание законодательства РФ. 2007. № 10. Ст. 1152.

ценных бумаг, акций (долей участия, паев в уставных (складочных) капиталах организаций) и об источниках получения средств, за счет которых совершена сделка, представляемых лицами, замещающими (занимающими) одну из должностей, указанных в пункте 1 части 1 статьи 2 Федерального закона от 03 декабря 2012 г. № 230-ФЗ – ст. 8 ФЗ «О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам»[1].

24. Конфиденциальность информации, относящейся к процедуре медиации – ст. 5 ФЗ «Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации)»[2].

25. Конфиденциальность третейского разбирательства – ст. 22 ФЗ «О третейских судах в Российской Федерации»[3].

26. Конфиденциальность информации о содержании корпоративного договора, заключенного участниками непубличного общества – ст. 67.2 Гражданского кодекса РФ (часть первая).

27. Конфиденциальность информации о новых решениях и технических знаниях, полученных сторонами по договору подряда – ст. 727 Гражданского кодекса РФ (часть вторая) Статья 771 Гражданского кодекса РФ (часть вторая).

28. Конфиденциальность сведений, касающихся предмета договоров на выполнение научно-исследовательских работ, опытно-конструкторских и технологических работ, хода их исполнения и полученных результатов, если иное не предусмотрено договорами Секрет производства (ноу-хау) – ст. 1465 Гражданского кодекса РФ (часть четвертая).

29. Запрет на распространение в средствах массовой информации, а также в информационно-телекоммуникационных сетях отдельных сведений

---

[1] О контроле за соответствием расходов лиц, замещающих государственные должности, и иных лиц их доходам: Федеральный закон от 03.12.2012 № 230-ФЗ (в ред. ФЗ от 03.11.2015 г. № 303-ФЗ) // Собрание законодательства РФ. – 2012. – № 50 (часть IV). – Ст. 6953.

[2] Об альтернативной процедуре урегулирования споров с участием посредника (процедуре медиации): Федеральный закон от 27.07.2010 № 193-ФЗ (в ред. ФЗ от 23.06.2013 г. № 233-ФЗ) // Собрание законодательства РФ. – 2010. – № 31. – Ст. 4162.

[3] О третейских судах в Российской Федерации: Федеральный закон от 24.07.2002 №102-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

Статья 4 Закона РФ от 27.12.1991 № 2124-1 «О средствах массовой информации», конфиденциальность информации, предоставляемой организациям (гражданам), осуществляющим производство и выпуск средств массовой информации – ст. 41 Закона РФ «О средствах массовой информации»[1].

30. Ограничение доступа к информации, входящей в состав кредитной истории, и (или) к коду субъекта кредитной истории – ст. 6 и 7 ФЗ «О кредитных историях»[2].

31. Конфиденциальность информации, предоставляемой эмитентами, профессиональным участникам рынка ценных бумаг, саморегулируемыми организациям профессиональных участников рынка ценных бумаг федеральному органу исполнительной власти по рынку ценных бумаг, конфиденциальность информации держателями реестра и депозитариями, конфиденциальность информации, полученной в связи с осуществлением функций трансфер-агента – ст. 8.1, 8.6, 44.1 ФЗ «О рынке ценных бумаг»[3], ст. 14 ФЗ «О центральном депозитарии»[4].

32. Конфиденциальность информации, предоставляемой клиринговым организациям и лицам, осуществляющим функции центрального контрагента – ст. 20 ФЗ «О клиринге и клиринговой деятельности»[5].

33. Конфиденциальность факта передачи в федеральный орган исполнительной власти, принимающий меры по противодействию легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма информации, указанной в пунктах 1 - 3 статьи 7.1-1 Федерального закона от 07.08.2001 N 115-ФЗ – ст. 7.1-1 ФЗ «О противодействии легализации

---

[1] О средствах массовой информации: Закон РФ от 27.12.1991 № 2124-1 (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

[2] О кредитных историях: Федеральный закон от 30.12.2004 № 218-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

[3] О рынке ценных бумаг: Федеральный закон от 22.04.1996 № 39-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

[4] О центральном депозитарии: Федеральный закон от 07.12.2011 № 414-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

[5] О клиринге и клиринговой деятельности: Федеральный закон от 07.02.2011 № 7-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

(отмыванию) доходов, полученных преступным путем, и финансированию терроризма»[1].

34. Конфиденциальность инсайдерской информации – ст. 6 ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»[2].

35. Конфиденциальность сведений, предоставляемых участниками торгов в соответствии с правилами организованных торгов – ст. 23 Федерального закона от 21.11.2011 № 325-ФЗ «Об организованных торгах»[3].

36. Конфиденциальность информации, полученной в связи с осуществлением деятельности по выдаче, погашению и обмену инвестиционных паев – ст. 28 ФЗ «Об инвестиционных фондах»[4].

37. Ограничение доступа к информации, полученной в ходе проведения проверок российских участников внешнеэкономической деятельности – ст. 17 ФЗ «Об экспортном контроле»[5].

38. Ограничение доступа к сведениям о результатах проведенной оценки уязвимости объектов транспортной инфраструктуры и транспортных средств, к сведениям, содержащимся в планах обеспечения транспортной безопасности объектов транспортной инфраструктуры и транспортных средств, к информационным ресурсам единой государственной информационной системы обеспечения транспортной безопасности – ст. 5, 9, 11 ФЗ «О транспортной

---

[1] О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма: Федеральный закон от 07.08.2001 № 115-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

[2] О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 27.07.2010 № 224-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. 2002. № 30. Ст. 3019.

[3] Об организованных торгах: Федеральный закон от 21.11.2011 № 325-ФЗ (с изм. от 03.07.2016 № 292-ФЗ) // Собрание законодательства РФ. 2011. № 48. Ст. 6726.

[4] Об инвестиционных фондах: Федеральный закон от 29.11.2001 № 156-ФЗ (в редакции от 03.07.2016. № 361-ФЗ) // Собрание законодательства РФ. 2001. № 49. Ст. 4562.

[5] Об экспортном контроле: Федеральный закон от 08.07.1999 №183-ФЗ (в редакции от 13.07.2015. № 216-ФЗ) // Собрание законодательства РФ от 26.07.1999 - № 30 - Ст. 3774.

безопасности»[1].

39. Конфиденциальность сведений, составляющих дактилоскопическую информацию – ст. 12 ФЗ «О государственной дактилоскопической регистрации в Российской Федерации[2].

40. Ограничение доступа к информации, содержащейся в контрольных измерительных материалах, используемых при проведении государственной итоговой аттестации – ст. 59 ФЗ «Об образовании в Российской Федерации»[3].

41. Ограничение доступа к сведениям о платежах в соответствующие бюджеты бюджетной системы Российской Федерации и об их плательщиках, поступающие в финансовые органы от органов Федерального казначейства – ст. 241 Бюджетного кодекса РФ[4].

42. Конфиденциальность сведений, содержащихся в индивидуальных лицевых счетах застрахованных лиц в системе обязательного пенсионного страхования – ст. 6 ФЗ «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования»[5].

43. Конфиденциальность информации, полученной негосударственным пенсионным фондом при обработке сведений, содержащихся в пенсионных счетах негосударственного пенсионного обеспечения, пенсионных счетах накопительной части трудовой пенсии и др. – ст. 15 ФЗ «О негосударственных пенсионных фондах»[6].

44. Конфиденциальность информации о получателе социальных услуг –

---

[1]О транспортной безопасности Федерального закона от 09.02.2007 № 16-ФЗ (с изм. от 06.07.2016 № 374-ФЗ) // Собрание законодательства РФ. - 2007 - № 7. - Ст. 837.

[2]О государственной дактилоскопической регистрации в Российской Федерации: Федеральный закон от 25.07.1998 № 128-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[3]Об образовании в Российской Федерации: Федеральный закон от 29.12.2012 № 273-ФЗ

[4]Бюджетный кодекс РФ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[5]Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования :Федеральный закон от 01.04.1996 № 27-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[6]О негосударственных пенсионных фондах: Федеральный закон от 07.05.1998 № 75-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

ст. 6 ФЗ «Об основах социального обслуживания граждан в Российской Федерации»[1].

45. Конфиденциальность сведений, содержащихся в Федеральной государственной информационной системе учета результатов проведения специальной оценки условий труда – ст. 18 ФЗ «О специальной оценке условий труда»[2].

46. Конфиденциальность сведений, ставших известными судебным приставам в связи с исполнением должностных обязанностей – ст. 6.4 ФЗ «Об органах принудительного исполнения Российской Федерации»[3].

47. Конфиденциальность информации, представляемой заинтересованным лицом в орган, проводящий расследования в целях принятия решения о целесообразности введения, применения, пересмотра или отмены специальной защитной меры, антидемпинговой меры или компенсационной меры – ст. 32 ФЗ «О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров»[4].

48. Конфиденциальность информации о членах политической партии, представляемой для сведения в уполномоченные органы – ст. 19 ФЗ «О политических партиях»[5].

49. Тайна исповеди – ст. 3 ФЗ «О свободе совести и о религиозных

---

[1]Об основах социального обслуживания граждан в Российской Федерации: Федеральный закон от 28.12.2013 №442-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[2]О специальной оценке условий труда: Федеральный закон от 28.12.2013 № 426-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

Об органах принудительного исполнения Российской Федерации: Федеральный закон от 21.07.1997 № 118-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[4]О специальных защитных, антидемпинговых и компенсационных мерах при импорте товаров: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[5]О политических партиях: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

объединениях»[1].

50. Конфиденциальность сведений о населении, содержащихся в переписных листах – ст. 8 ФЗ «О Всероссийской переписи населения»[2].

51. Ограничение доступа к сведениям, содержащимся в переписных листах об объектах сельскохозяйственной переписи – ст. 12 ФЗ «О Всероссийской сельскохозяйственной переписи»[3].

52. Ограничение доступа к первичным статистическим данным, содержащимся в формах федерального статистического наблюдения – ст. 9 ФЗ «Об официальном статистическом учете и системе государственной статистики в Российской Федерации»[4].

53. Ограничение доступа к информации, содержащейся в паспортах безопасности объектов топливно-энергетического комплекса – ст. 8 ФЗ «О безопасности объектов топливно-энергетического комплекса»[5].

54. Конфиденциальность информации, полученной членами саморегулируемой организации в области энергетического обследования в ходе проведения энергетического обследования – ст. 18 ФЗ «Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации»[6].

---

[1]О свободе совести и о религиозных объединениях: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[2]О Всероссийской переписи населения: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[3]О Всероссийской сельскохозяйственной переписи: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[4]Об официальном статистическом учете и системе государственной статистики в Российской Федерации: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[5]О безопасности объектов топливно-энергетического комплекса: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

[6]Об энергосбережении и о повышении энергетической эффективности и о внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 08.12.2003 № 165-ФЗ (в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

55. Конфиденциальность сведений, содержащихся в заявках на участие в конкурсе на право заключить контракт на проведение лотерей – ст. 24.10 ФЗ «О лотереях»[1].

Интерес в этом случае вызывает то, что если информация не отнесена к категории сведений ограниченного доступа и в отношении владельца этой информации совершаются действия по ее завладению, то подобного рода деяния не входят в сферу уголовно-правовой охраны и не могут квалифицироваться по ст. 272 УК РФ.

[1]О лотереях: Федеральный закон от 11.11.2003 № 138-ФЗ в ред. ФЗ от 29.12.2015 г. № 382-ФЗ) // Собрание законодательства РФ. – 2002. – № 30. – Ст. 3019.

Приложение 2.

АНКЕТА
для следователей и оперуполномоченных органов внутренних дел, специализирующихся на расследовании преступлений в сфере информационных технологий

Уважаемые коллеги! Просим Вас ответить на следующие вопросы анкеты, поставив любой знак рядом с подходящим вариантом ответа. Если Вы не согласны ни с одним из вариантов, предложите свой ответ.

1. Где, по Вашему мнению, может находиться компьютерная информация:

1) Компьютер
2) Телефон
3) Интернет-сайт
4) Учетная запись в социальной сети
5) Компьютерная программа
6) другое_____

2. Какие по Ваше мнению преступления вызывают сложности при выявлении, раскрытии и расследовании:

1) Кардинг
2) Скимминг
3) Неправомерный доступ к компьютерной информации
4) Использование вредоносных компьютерных программ
5) Мошенничество в сфере компьютерной информации

В чем проявляются трудности:_____

3. Каковы на Ваш взгляд причины и условиями совершения преступлений в сфере обращения охраняемой законом информации:

1. Рост числа пользователей и как следствие увеличение объемов обрабатываемой и хранимой информации.
2. Недостаточность мер по защите компьютерной информации.
3. Другое_____

4. Каковы на Ваш взгляд мотивы совершения преступлений в сфере обращения охраняемой законом информации:

1) Корысть
2) Желания попробовать свои знания
3) Личные мотивы (месть, зависть и т.п.)
4) Другое_____

5. Считаете ли Вы, что неправомерный доступ к охраняемой законом информации следует относить к преступлению?

1) да
2) нет, необходимо декриминализовать подобные деяния и предусмотреть административную ответственность за их совершение
3) другое_____

6. Можно ли, на Ваш взгляд, считать преступлением неправомерный доступ к охраняемой законом информации путем взлома интернет-страницы (аккаунта) в социальных сетях (vk.com, ok.ru и др.)?

1) да, независимо от наступления последствий
2) нет
3) да, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации
4) другое_____

7. Считаете ли Вы необходимым принятие закона, в котором будет предусмотрен механизм закрытия интернет-ресурсов, на которых размещаются вредоносные программы, информация о способах совершения компьютерных преступлений и т.п.?
1) да
2) нет
3) другое_____

8. Как Вы думаете, есть ли необходимость усилить уголовную ответственность за преступления в сфере охраняемой законом информации?

1) да
2) нет
3) другое_____

9. По Вашему мнению, есть ли необходимость снизить возраст привлечения к уголовной ответственности за преступления в сфере охраняемой законом информации с 16 до 14 лет?

1) да
2) нет
3) другое_____

10. Как на Ваш взгляд было бы правильнее называть главу 28 УК РФ:

1) Преступления в сфере компьютерной информации
2) Преступления в сфере цифровой информации
3) Преступления в сфере электронной информации
4) Преступления в сфере обращения информации
4) другое_____

11. На Ваш взгляд, есть ли необходимость введения в школах курса по безопасности в Интернете?

1) да
2) нет
3) другое_____

12. На Ваш взгляд, необходимо ли предусмотреть курс по квалификации и расследованию компьютерных преступлений в рамках обучения по повышению квалификации для сотрудников правоохранительных органов?

1) да
2) нет
3) другое_____

13. Какие по Вашему мнению необходимо предпринять действия в целях уголовно-правового и криминологического противодействия преступлениям в сфере охраняемой законом информации:

_____
_____

14. В результате чего выявляется факты совершения преступлений в сфере охраняемой законом информации:
    1) В ходе расследования других видов преступлений
    2) Случайно
    3) Агентурная работа
    4) При проведении ОРМ по проверкам заявлений граждан
    5) В результате проверок организаций собственными службами безопасности
    6) Другое _____

15. Какой термин шире по содержанию и охватывает все случаи неправомерного воздействия на информацию:

    1) «охраняемая законом информация»
    2) «компьютерная информация»
    3) «электронная информация»
    4) «цифровая информация»