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

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Новосибирск – 2021

Работа выполнена в федеральном государственном казенном образовательном учреждении высшего образования «Восточно-Сибирский институт Министерства внутренних дел Российской Федерации», на кафедре уголовного права и криминологии.

Научный руководитель: Заслуженный юрист Российской Федерации,
доктор юридических наук, профессор
Репецкая Анна Леонидовна

Официальные оппоненты:

Ефремова Марина Александровна, доктор юридических наук, Казанский филиал федерального государственного бюджетного образовательного учреждения высшего образования «Российский государственный университет правосудия», профессор кафедры уголовно-правовых дисциплин

Евдокимов Константин Николаевич, кандидат юридических наук, доцент, Иркутский юридический институт (филиал) федерального государственного казенного образовательного учреждение высшего образования «Университет прокуратуры Российской Федерации», доцент кафедры гражданско-правовых дисциплин

Ведущая организация:

Федеральное государственное бюджетное образовательное учреждение высшего образования «Омский государственный университет им. Ф.М. Достоевского»

Защита состоится 26 ноября 2021 г. в 11.00 час. на заседании объединенного совета по защите диссертаций на соискание ученой степени кандидата наук, на соискание ученой степени доктора наук Д 999.126.03 на базе ФГАОУ ВО «Новосибирский национальный исследовательский государственный университет» по адресу: г. Новосибирск, Академгородок, ул. Пирогова, 1, корп. Ректорат, ауд. 414, зал заседаний Ученого совета НГУ.

С диссертацией можно ознакомиться в научной библиотеке НГУ и на сайте: https://www.nsu.ru; https://www.dvfu.ru; http://sfu-kras.ru

Автореферат разослан «___» _____ 20___ г.

Учёный секретарь
диссертационного совета Коротких Н.Н.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

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, посягающих 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; существуют противоречия в диспозициях уголовно-правовых норм, их регламентирующих. В современной 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, предмета 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.

Большой вклад в исследование различных аспектов противодействия преступлениям в сфере компьютерной информации был сделан такими

---

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

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

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 характера, 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[3] (10 %); скимминг[4] (9 %); наименее распространенным способом совершения была ddos-атака[5] – 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 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

[3] 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)

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

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

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 гг.;

– 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.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обосновываются выбор темы диссертационной работы, ее актуальность и степень научной разработанности; определяются цели, задачи, научная новизна, теоретическая и практическая значимость работы, методология исследования; формулируются основные положения, выносимые на защиту; указывается степень достоверности результатов проведенных исследований и эмпирическая база исследования; приводятся сведения об апробации результатов исследования.

Первая глава – «Теоретические основы изучения преступлений в сфере обращения охраняемой законом информации» – состоит из двух параграфов. В первом параграфе «*Понятие охраняемой законом информации*» уточняется уголовно-правовая природа исследуемого феномена. Соискателем проведен анализ определений «аналоговая информация», «компьютерная информация», «электронная информация», «цифровая информация», «охраняемая законом информация», как предмета преступления. На его основе сделал вывод, что понятие «охраняемая законом информация», применяемое в рамках науки уголовного права, за нарушения оборота которой предусмотрена уголовная ответственность, включает в себя объем понятий «аналоговая информация», «цифровая информация», «компьютерная информация», «электронная информация», то есть является родовым по отношению к ним. Учитывая, что информация ограниченного доступа в любом ее виде должна охраняться законом, нет необходимости выделения из нее отдельной категории в виде компьютерной, электронной или цифровой информации. Уточняется, что «пользовательская информация» (фотографии, ФИО, дата рождения, адрес проживания, телефон, интересы, поисковые запросы и т.д.) стала разновидностью охраняемой законом информации и она нуждается в уголовно-правовой охране.

Таким образом, 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 как предмет преступного посягательства – это сведения, на которые распространяется режим ограниченного доступа, установленный Конституцией РФ и Федеральными законами, и защищенные владельцем информации от неправомерного доступа.

Второй параграф «*Общая характеристика преступлений в сфере обращения охраняемой законом информации, их понятие и виды*» посвящен исследованию имеющихся подходов к определению рассматриваемого понятия в юридической науке, в частности соотношению понятий «компьютерное преступление», «киберпреступление», на основе которого автор приходит к выводу, что под преступлениями в сфере обращения охраняемой законом информации необходимо понимать виновно совершенное общественно опасное деяние, посягающее на общественные отношения, возникающие по поводу охраны информации ограниченного доступа. При этом можно выделить главные свойства указанного вида информации: владелец информации предпринял действия по защите информации; информация подпадает под сведения ограниченного доступа, режим оборота которой регулируется Конституцией РФ или Федеральными законами. Классификация преступлений в сфере обращения охраняемой законом информации в зависимости от способа совершения противоправного деяния позволяет выделить 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.

Вторая глава «Уголовно-правовая характеристика преступлений в сфере обращения охраняемой законом информации» состоит из двух параграфов. В первом параграфе «*Юридический анализ основных составов преступлений в сфере обращения охраняемой законом информации*» рассмотрены уголовно-правовые признаки основных составов преступлений в сфере охраняемой законом информации, в том числе общественно опасные последствия, выражающиеся в форме копирования, блокирования и модификации информации. В результате чего сделан 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.

Исходя из изложенного, предлагается 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.

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 не наносят вред обладателю информации. Также в УК РФ необходимо закрепить понятия «блокирование», «модификация», «уничтожение» электронной информации.

Во втором параграфе «*Проблемы квалификации и отграничения от смежных составов преступлений в сфере обращения охраняемой законом информации*» проведен анализ основных составов преступлений в сфере охраняемой законом информации, результат которого 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, однако направлены на доступ в том или ином виде к охраняемой законом информации.

Предлагается перенести в сферу уголовного проступка (если, конечно, закон об уголовном проступке будет принят) или в разряд административного правонарушения преступления в сфере обращения охраняемой законом информации без наступления последствий в виде копирования, блокирования,

модификации, а также за неправомерный доступ к охраняемой законом информации, если эти действия не причинили моральные страдания потерпевшему или не совершены из корыстной заинтересованности либо мести.

Третья глава «Криминологическая характеристика преступлений в сфере обращения охраняемой законом информации» состоит из трех параграфов.

В первом параграфе «*Состояние, структура и динамика преступлений в сфере обращения охраняемой законом информации*» проанализированы количественный и качественный показатели состояния и структуры указанных преступлений. Статистические сведения Главного информационно-аналитического центра МВД России отражают ежегодное снижение количества зарегистрированных преступлений в сфере компьютерной информации. Однако за чертой уголовной статистики остается значительное число скрытых, латентных преступлений, число которых значительно выше данных официальной статистики.

В работе проанализированы материалы уголовных дел по преступлениям в сфере обращения охраняемой законом информации. Результат позволил автору предложить структуру преступлений в сфере обращения охраняемой законом информации по способам их совершения: использование вредоносных компьютерных программ для мобильных телефонов – 55 %; использование вредоносных компьютерных программ для неправомерного доступа к компьютерной технике (персональный компьютер, мобильный компьютер и т.п.) – 11 %; неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам – 11 %; кардинг - 10 %; скимминг – 9 %; ddos-атака – 4 %.

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.

Второй параграф носит название «*Личность преступника, совершающего преступления в сфере обращения охраняемой законом информации*». В качестве эмпирической базы исследования использовались сведения о 120 лицах, осужденных за совершение преступлений в сфере обращения охраняемой законом информации.

Преступления в указанной сфере совершают лица мужского пола, среди которых преобладают молодые люди в возрасте от 19 до 24 лет (56,1 %), средний возраст преступников составил 26 лет, доля женщин составляет 1 %. 64,7 % – с высшим и средним образованием. По роду занятий 21,7 % – это учащиеся и студенты (все – мужчины), 9,4 % – программисты (все – мужчины), 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.

Большинство преступников проживали в крупных городах – центрах субъектов Российской Федерации – 73,1 %. Обычно преступления в сфере компьютерной информации совершаются в одиночку, так совершено (85,6 %), в соучастии совершено 14,4 % преступлений. Подавляющее большинство преступников (87 %) знали об ответственности за совершение преступлений в сфере электронной информации, однако частная превенция здесь не сработала. У этих людей не были сформированы позитивные убеждения, взгляды и нормы морали. 13 % преступников пояснили, что не догадывались о том, что совершают преступления в сфере электронной информации. К лицам, совершающим преступления в сфере обращения охраняемой законом информации, применим термин «информационные воры», целью которых является похищение 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, члены которой зачастую находятся в разных регионах нашей страны или за ее пределами. Однако в цифрах официальной статистики данный факт не нашел своего отражения. Автор делает вывод о том, что это связано, во-первых, со сложностью выявления преступных связей субъекта преступления; во-вторых, со сложностью доказывания формы соучастия в преступлении, что обусловлено использованием мессенджеров с шифрованием электронных сообщений, общение на форумах в сети ТОР, использованием криптовалют для распределения дохода, полученного преступным путем.

Предложена классификация лиц, совершающих преступления в сфере обращения охраняемой законом информации, и дана их характеристика:

1. *Лица, использующие вредоносные компьютерные программы для мобильных телефонов:* непосредственно вирусописатель; «заливщик»; лицо, администрирующие Интернет-ресурс, на котором отображаются данные о «зараженных» устройствах (администратор); «дроп»; организатор

2. *Лица, использующие вредоносные компьютерные программы для неправомерного доступа к компьютерам, ноутбукам и т.д.*

3. *Лица, осуществляющие неправомерный доступ к учетным записям в социальных сетях и электронным почтовым ящикам*.

4. *Кардеры*.

5. *Лица, совершающие хищение денежных средств, используя «Скиммер»*.

6. *Лица, осуществляющие Ddos-атаки.*

В третьем параграфе «*Факторы, детерминирующие совершение преступлений в сфере обращения охраняемой законом информации*» исследуются детерминанты девиантного поведения, связанного с совершением преступлений в сфере обращения охраняемой законом информации. Делается вывод о том, что детерминанты указанных преступлений имеют многофакторный характер, к ним относятся: факторы правового характера, технические, организационные, виктимологические.

Сделан вывод о том, что существование преступности в сфере оборота охраняемой законом информации определяется несколькими специфическими факторами, которые не совпадают с факторами, порождающими преступность в целом. К таким факторам можно отнести: факторы правового характера технические факторы, организационные факторы, социально-экономические факторы, виктимологические факторы.

Четвертая глава «Предупреждение преступлений в сфере обращения охраняемой законом информации» состоит из двух параграфов, в которых предлагаются меры профилактического характера, базирующиеся на результатах диссертационного исследования.

В первом параграфе «*Уголовно-правовые меры предупреждения преступлений в сфере обращения охраняемой законом информации*» на основе юридического анализа обосновываются и вносятся предложения по совершенствованию уголовного законодательства в процессе регламентации ответственности за совершение преступлений в сфере обращения охраняемой законом информации.

Указывается на отсутствие должного государственного регулирования за пунктами коллективного доступа в сеть Интернет, которое позволяет киберпреступникам скрывать свою личность, что затрудняет выявление виновных лиц. Отсюда следует необходимость введения административной ответственности по отношению к владельцам пунктов коллективного доступа в сеть Интернет, которые игнорируют правила авторизации пользователей, а также законодательное закрепление обязанности владельцев пунктов коллективного доступа к сети Интернет производить сбор сведений о клиентах с обязательным предъявление документа, удостоверяющего личность, актуального телефонного номера.

Автором обосновываются предложения дополнить гл. 28 УК РФ статьей «Незаконное ограничение доступа к информации, находящейся в телекоммуникационных сетях, с использованием вредоносных компьютерных программ», дополнить ст.ст. 272-274[1] УК РФ общественно опасными последствиями в виде ознакомления с информацией ограниченного доступа, а

также отграничить преступление от административного проступка: доступ к цифровой информации, повлекший копирование, блокирование, уничтожение, ознакомление, если эти действия причинили моральные страдания или из корыстной заинтересованности, мести.

Второй параграф носит название «*Иные специально-криминологические меры предупреждения преступлений в сфере обращения охраняемой законом информации».* Делается вывод о том, что необходимо включить сайты, на которых происходит общение лиц, интересующихся преступлениями в сфере обращения охраняемой законом информации, в реестр запрещённых сайтов, наряду с порнографическими сайтами, сайтами по пропаганде наркотиков и т.д. Под влиянием негативного информационного потока и обещания быстрого обогащения при совершении преступлений в сфере обращения охраняемой законом информации у лица может возникнуть мотив для совершения преступления.

Предлагается запретить операторам связи использовать «серые» IP-адреса, то есть публичные сетевые адреса, преобразованные по технологии NAT (Network Address Translation). Благодаря этой технологии один IP-адрес может одновременно предоставлен нескольким абонентам или устройствам, количество которых может доходить до нескольких тысяч. Так как большинство преступлений в сфере компьютерной 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 ввиду сложности их изобличения. Предлагается законодательно запретить операторам связи использовать протокол «Ipv4», а как альтернативу применять протокол «IPv6». Внедрение нового протокола может способствовать борьбе с преступлениями в сфере компьютерной информации в силу более точного выявления абонента, оставляющего электронные следы в сети Интернет.

В **заключении** в обобщенном виде излагаются основные положения,

выводы, предложения, сформулированные в ходе диссертационного исследования, а также рекомендации по совершенствованию уголовного законодательства Российской Федерации в сфере борьбы с преступлениями рассматриваемой категории.

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.

Рекомендации и перспективы дальнейшей разработки темы исследования. 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. 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.

Основные положения диссертационного исследования отражены в следующих публикациях автора:

Статьи в ведущих рецензируемых научных журналах, рекомендованных Высшей аттестационной комиссией при Минобрнауки России для опубликования основных научных результатов диссертаций:

1. Родивилин, И.П. Незаконное ограничение доступа к компьютерной информации в сети Интернет: уголовно-правовой аспект / И.П. Родивилин, А.Л. Репецкая // Библиотека уголовного права и криминологии, 2016. – № 3 (15). – С. 79–84 (0,4 п.л./0,4 п.л.).

2. Родивилин, И.П. Уголовно-правовое и криминологическое противодействие Вэб-кардингу / И.П. Родивилин // Библиотека уголовного права и криминологии, 2017. – № 1 (19). – С. 127–131 (0,5 п.л.).

3. Родивилин, И.П. Типологизация лиц, совершающих преступления в сфере компьютерной информации, по способу преступного деяния / И.П. Родивилин // Научный вестник Омской академии МВД России. – Омск, 2017. – № 4. – С. 25–29 (0,7 п.л.).

4. Родивилин, И.П. Интеллектуальный разврат несовершеннолетних в сети Интернет / И.П. Родивилин, В.В. Коломинов, Д.Э. Брыжак // Сибирские уголовно-процессуальные и криминалистические чтения. 2020. – № 1. – С. 64-76 (0,4 п.л./0,2 п.л./0,2 п.л.).

5. 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 (0,8 п.л.).

6. Родивилин, И.П. Современная специфика детерминации преступлений в сфере обращения охраняемой законом информации // Вестник УДГУ. – 2021. – №2. – С. 305-311 (0,8 п.л.).

Иные публикации:

7. Родивилин, И.П. Лицензирование в области защиты информации как форма защиты интересов гражданина, общества и государства / И.П. Родивилин //

Правозащитная деятельность органов государственной власти: проблемы и перспективы: материалы круглого стола с междунар. участием. – Иркутск, 2012. – С. 109-112. (0,3 п.л.).

8. Родивилин, И.П. Проблемы квалификации преступлений в сфере компьютерной информации, совершаемых с использованием дистанционного управления банковским счетом и их предупреждение / И.П. Родивилин // Пролог: журнал о праве. – Иркутск, 2014. – № 2 (6). – С. 61–64 (0,3 п.л.).

9. Родивилин, И.П. К вопросу о квалификации преступлений в сфере компьютерной информации, совершаемых с помощью компьютерных технологий / И.П. Родивилин // Уголовный закон Российской Федерации: проблемы правотворчества и перспективы совершенствования: мат-лы Всероссийского круглого стола. – Иркутск, 2014. – № 5. – С. 192–196 (0,3 п.л.).

10. Родивилин, И.П. Проблемы охраны конституционных прав, предусмотренных статьей 23 Конституции РФ / И.П. Родивилин // 20 лет Конституции России: актуальные проблемы развития правового государства: сб. науч. тр.– Иркутск, 2014. – С. 188–192 (0,2 п.л.).

11. Родивилин, И.П. Значение субъективной стороны в составах преступлений в сфере компьютерной информации / И.П. Родивилин // Juris Prudentia. – Иркутск, 2015. – Т. 3. № 1. – С. 10 (0,2 п.л.).

12. Родивилин, И.П. Уголовно-правовое противодействие незаконному ограничению доступа к компьютерной информации в сети Интернет / И.П. Родивилин, А.А. Шаевич // Криминалистические чтения на Байкале – 2015: материалы междунар. науч.-практ. конф. – Иркутск, 2015. – С. 275–278. – (0,3 п.л./0,2).

13. Родивилин, И.П. Преступления в сфере компьютерной информации: состояние, динамика, тенденции, особенности личности преступника / И.П. Родивилин // Проблемы современного российского законодательства: материалы III Всеросс. науч.-практ. конф. – Иркутск, 2015. – С. 310–312 (0,2 п.л.).

14. Родивилин, И.П. Использование компьютерной информации при раскрытии и расследовании преступлений, совершенных с использованием сети

Интернет / И.П. Родивилин // Криминалистика: вчера, сегодня, завтра: сб. науч. тр.– Иркутск, 2015. – Вып. 3–4. – С. 173–178 (0,5 п.л.).

15. Родивилин, И.П. Уголовно-правовое противодействие незаконному ограничению доступа к компьютерной информации в сети Интернет / И.П. Родивилин, А.А. Шаевич // Криминалистические чтения на Байкале – 2015: материалы междунар. науч.-практ. конф. – Иркутск, 2015. – С. 275–278 (0,3 п.л./0,2).

16. Родивилин, И.П. Участие специалиста в раскрытии и расследовании киберпреступлений / И.П. Родивилин, А.А. Шаевич // Проблемы современного российского законодательства: материалы IV Всерос. науч.-практ. конф. – Иркутск, 2015. – С. 316–319 (0,2 п.л./0,1 п.л).

17. Родивилин, И.П. Использование электронной информации при раскрытии и расследовании преступлений / И.П. Родивилин, В.А. Родивилина // Проблемы современного российского законодательства: материалы IV Всерос. науч.-практ. конф. – Иркутск, 2015. – С. 305–308 (0,4 п.л./0,2 п.л.).

18. Родивилин, И.П. К вопросу о личности преступника, совершающего преступления в сфере компьютерной информации / И.П. Родивилин, В.А. Родивилина // Уголовный закон Российской Федерации: проблемы правоприменения и перспективы совершенствования: материалы науч.-практ. конф. – Иркутск, 2017. – С. 188–191 (0,1 п.л./0,1 п.л.).

19. Родивилин, И.П. Цифровое неравенство – угроза безопасности Российской Федерации / И.П. Родивилин // Проблемы обеспечения национальной безопасности Российской Федерации: материалы науч.-практ. конф. – Иркутск, 2017. – С. 139–143 (0,3 п.л.).

20. Родивилин, И.П. Криптовалюта как объект преступления / И.П. Родивилин // Деятельность правоохранительных органов в современных условиях: материалы междунар. науч.-практ. конф. – Иркутск, 2018. – С. 262-265 (0,3 п.л.).

21. Родивилин, И.П. Информационное оружие // Евразийский интеграционный проект: цивилизационная идентичность и глобальное

позиционирование: материалы междунар. науч.-практ. конф. – Иркутск, 2018. – С. 275-278 (0,3 п.л.).

22. Родивилин, И.П. Защита цифровых прав человека // Конституция Российской Федерации и правовая политика на современном этапе: материалы всероссийской. науч.-практ. конф. – Иркутск, 2019. – С. 275-278 (0,4 п.л.).