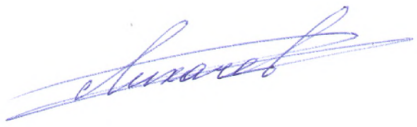
На правах рукописи



Лихачев Никита Александрович

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАКОНОДАТЕЛЬНЫЙ, ПРАВОПРИМЕНИТЕЛЬНЫЙ И ДОКТРИНАЛЬНЫЙ АСПЕКТЫ

Специальность 5.1.4. Уголовно-правовые науки
(юридические науки)

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Краснодар – 2024

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Кубанский государственный университет»

Научный руководитель: **Прохоров Леонид Александрович**
доктор юридических наук, профессор,
заслуженный юрист РФ
заслуженный работник высшей школы РФ,

Официальные оппоненты: **Русскевич Евгений Александрович,**
доктор юридических наук, доцент,
ФГАОУ ВО «Московский государственный юридический университет имени О.Е. Кутафина (МГЮА)», профессор кафедры уголовного права

Соловьев Владислав Сергеевич,
кандидат юридических наук, доцент,
ФГКОУ ВО «Краснодарский университет Министерства внутренних дел Российской Федерации», начальник кафедры уголовного права и криминологии

Ведущая организация: федеральное государственное автономное образовательное учреждение высшего образования «Дальневосточный федеральный университет»

Защита состоится «27» июня 2024 года в 10 часов 00 минут на заседании диссертационного совета 24.2.320.07 по юридическим наукам, созданного на базе ФГБОУ ВО «Кубанский государственный университет» по адресу: 350000, г. Краснодар, ул. Рашпилевская, 43, ауд. 11.

С диссертацией и авторефератом можно ознакомиться в научной библиотеке и на официальном сайте ФГБОУ ВО «Кубанский государственный университет» (https://www.kubsu.ru/).

Автореферат разослан «___» мая 2024 г.

Ученый секретарь
диссертационного совета 24.2.320.07
кандидат юридических наук, доцент Лукожев Хусен Манаевич

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования обусловлена существенными изменениями, происходящими в общественных отношениях, вызванными процессами цифровизации и информатизации. Урбанизация, внедрение новых технологий привели к появлению большого количества альтернативных носителей информации – электронных денег, паспортов, акций, биометрических данных, иных документов, в том числе и QR-кодов, содержащих основные персональные данные пользователей. К сожалению, любые передовые технологии практически сразу начинают использоваться в преступной деятельности. Статистические показатели совершаемых уголовно-правовых деликтов в сфере информационных и компьютерных технологий стали расти, а законодательство и правоохранительные органы зачастую не успевают реагировать на стремительно меняющуюся структуру общественных отношений.

По данным Главного информационно-аналитического центра Министерства внутренних дел Российской Федерации «О состоянии преступности в России», в 2018 г. было зарегистрировано 174674 преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, раскрыто – 43362[1]. В 2019 г. – уже 294409 преступлений, из них раскрыто – 65238[2]. В 2020 г. зарегистрировано 510396 названных преступлений, раскрыто 94942. В 2021 г. эти показатели составили 517722 и 118920 соответственно, в 2022 г. – 522065 и 142384. В 2023 г. каждое третье преступление совершалось с использованием информационно-телекоммуникационных технологий. В этой сфере было зарегистрировано на 29,7% больше уголовно наказуемых деяний, чем в январе-декабре 2022 г., при этом названных преступлений в .2023 г. раскрыто на 21% больше, чем в предыдущем[3]. Как отмечается в отчетах МВД РФ, их профилактика по-прежнему остается одной из важнейших задач органов внутренних дел[4].

Очевидно, что информационная безопасность в ближайшее время станет одним из важнейших объектов уголовно-правовой охраны. Коммуникационная индустрия стремительно развивается, ее доля в общественных процессах, в экономике и социальной жизни занимает ключевую роль. Об этом еще в 2016 г. в Послании Федеральному Собранию Российской Федерации отмечал Президент РФ В.В. Путин[5]. Практически у каждого гражданина есть свой аккаунт в социальных сетях, онлайн-счет в банке, а его персональные данные собирают различные сайты в коммерческих целях, формируя тем самым частные базы данных. Некоторые совершают более радикальные действия, осуществляя сбор данных о физических и юридических лицах для дальнейшей их реализации в коммерческих целях (в частности, различные телеграмм-каналы[6]).

---

[1] Статистика и аналитика МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/16053092/ (дата обращения: 14.02.2024 г.)..

[2] Статистика и аналитика МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/19412450/ (дата обращения: 14.02.2024 г.).

[3] Статистика и аналитика МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/22678184/ (дата обращения: 14.02.2024 г.).

[4] См.: Краткая характеристика состояния преступности в Российской Федерации за январь – декабрь 2023 года. URL: https://мвд.рф/reports/item/47055751/ (дата обращения: 14.02.2024 г.).

[5] Послание Президента Российской Федерации Федеральному Собранию Российской Федерации 01 декабря 2016 г. URL: http://kremlin.ru/events/president/ news/53379 (дата обращения: 14.01.2023 г.).

[6] Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации. URL: https://rkn.gov.ru/news/rs c/news73728.htm (дата обращения: 14.01.2023 г.).

Информационное пространство, ИТС «Интернет» стали базисными площадками для экономических отношений и процессов. Так, за 2020 г. доходы в бюджет от экономической деятельности российского сегмента ИТС «Интернет» составили более 7 трлн. руб.[1]

Процессы коммуникаций стремительно ускоряются, а средства хранения информации (компьютеры, телефоны, планшеты и т.д.) становятся источниками, содержащими практически все сведения о частной жизни лица, его банковской, семейной, личной, медицинской тайне. Так, формирование устойчивого информационного общества, рост преступлений актуализирует для государства задачи по обеспечению информационной безопасности, защите информации и персональных данных граждан. Принятая Указом Президента РФ № 400 в 2021 г. новая Стратегия национальной безопасности выделяет обеспечение информационной безопасности как одно из приоритетных направлений государственной деятельности, обосновывая это возникновением ряда внешних и внутренних угроз[2]. В рамках реализации данного направления в 2016 г. Указом Президента РФ № 646 принята Доктрина информационной безопасности Российской Федерации, в которой отмечается важность использования и формирования правовых (в том числе уголовно-правовых) основ обеспечения информационной безопасности[3].

В 2021 г. был принят еще один нормативный акт – Основы государственной политики Российской Федерации в области международной информационной безопасности, в котором отмечается необходимость внедрения международных правовых стандартов в области обеспечения информационной безопасности на уровне различных международных организаций[4].

Современная редакция Уголовного кодекса Российской Федерации (далее – УК РФ) предусматривает составы преступлений, посягающих на информацию, в частности, они представлены в отдельной гл. 28 УК РФ «Преступления в сфере компьютерной информации». Тем не менее, существует ряд практических и теоретических проблем, требующих пристального научного внимания и детального исследования. Неизбежный количественный и качественный рост информационных правоотношений является значимой причиной, благодатной почвой для «киберпреступности», появления новых уголовно-правовых деликтов в исследуемой сфере.

Отдельно возникает необходимость обеспечения информационной безопасности путем непосредственной уголовно-правовой защиты специальных технических средств, создающих условия для бесперебойного функционирования ИТС «Интернет», государственных цифровых систем, учета

---

[1] Видеообращение председателя правительства РФ М.В. Мишустина к участникам 13-й Недели российского интернета – RIW 20/21 URL: http://government.ru/news/44012/ (дата обращения: 14.01.2023 г.).

[2] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02 июля 2021 г. № 400 // СПС «КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения: 14.01.2023 г.).

[3] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05 декабря 2016 г. № 646 // СПС «КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/ (дата обращения: 14.01.2023 г.).

[4] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности: Указ Президента РФ от 12 апреля 2021 г. № 213 // СПС «КонсультантПлюс URL: http://www.consultant.ru/document/cons_doc_LAW_381999/9bbf31c7586971ae3d3076bfb49080d41d6c4484 (дата обращения: 14.01.2023 г.).

баз данных и т.д. К данной сфере относятся и объекты энергетической инфраструктуры – электростанции, кабели, серверы, физически осуществляющие функционирование киберпространства.

Особо следует указать на проблему терминологического характера, а именно на наличие различных понятий, неоднозначно и по-своему трактующих преступления в информационной среде – «киберпреступления», преступления против компьютерной информации, информационные преступления и т.д., что требует предметного анализа и универсализации. Безусловно, проблема обеспечения информационной безопасности уголовно-правовыми средствами носит комплексный характер. В связи с этим возникает необходимость формирования единого подхода к противодействию преступлениям, связанным с посягательствами на информацию. Именно системный, научно-обоснованный подход должен лечь в основу развития уголовно-правового противодействия преступлениям в сфере информационной безопасности, необходимость которого отмечается многими учеными и практиками. Поэтому уголовно-правовая охрана информации, уголовно-правовое противодействие в сфере обеспечения информационной безопасности и защиты информации является одной из наиболее актуальных проблем в науке уголовного права.

Степень научной разработанности темы исследования. Проблематика уголовно-правовой охраны и обеспечения национальной безопасности Российской Федерации в научной среде представлена достаточно широко, однако большинство работ имеет разносторонний характер, и их авторы не придерживаются единого мнения.

К вопросам обеспечения информационной безопасности, к анализу информационных войн обращались в своих работах Н.П. Арапов, Е.И. Галяшина, А.Б. Губарев, В.Д. Никишин и ряд иных авторов.

Ключевые проблемы информационного права, теории информации и кибернетики, определения сущности информации раскрываются в трудах Н.М. Амосова, И.А. Артеменко, Н. Винера, Ю.В. Волкова, В.М. Глушкова, К. Шеннона и др.

Проблемам уголовно-правового обеспечения информационной безопасности и ее уголовно-правовой охраны посвящены работы Р.Г. Асланяна, А.Г. Волеводза, Р.Р. Гайфутдинова, К.Н. Евдокимова, Т.В. Закупень, Д.А. Калмыкова, В.Н. Лопатина, А.А. Малюка, Е.А. Русскевича, В.Г. Степанова-Егиянца и др.

Уголовно-правовой охране общественных информационных отношений уделено внимание в трудах И.Р. Бегишева, Р.И. Дремлюги, А.Б. Губарева, М.А. Ефремовой, Д.Н. Карпова, А.И. Коробеева, Э.Л. Кочкина, В.Н. Куфлевой, В.А. Номоконова, Л.А. Прохорова и др.

Криминологические аспекты преступности в сфере обеспечения информационной безопасности анализировались И.Р. Бегишевым, В.Ф. Джафарли, С.Г. Никитиным, Е.А. Маслаковой, В.С. Овчинским, А.В. Петровским, В.С. Соловьевым, З.И. Хисамовой и др.

Международные аспекты уголовно-правового обеспечения информационной безопасности разрабатывались такими представителями отечественной науки, как Е.С. Зиновьева, В.П. Коняхин, А.В. Крутских, В.А. Мазуров, Д.П. Потапов, В.В. Сорокин и др.

Необходимо отметить значимость исследований, проведенных указанными авторами, так как они сформировали сущностные основы уголовно-правовой охраны информационной безопасности в Российской Федерации. При этом информационное пространство, равно как и современное уголовное законодательство, претерпело существенные изменения. По различным

подсчетам, в уголовный закон с момента принятия в 1996 г. было внесено более 1000 изменений, что не могло не сказаться на его единообразии. Поэтому проблема формирования единой уголовно-правовой политики в сфере обеспечения информационной безопасности так и не решена, не сложился единый подход к уголовно-правовой охране информации, не разработано определение информационной безопасности как объекта уголовно-правовой охраны, отсутствует официально-правовое определение «компьютерных преступлений», «информационных преступлений», «киберпреступлений», конфиденциальных сведений, хищения информации и т.д. Это позволяет заключить об отсутствии системного подхода к формированию уголовно-правовой политики в сфере обеспечения информационной безопасности и защиты информации, что требует дальнейшего исследования и изучения.

Действующее законодательство претерпевает значительные изменения, связанные с модернизацией норм, направленных на уголовно-правовую защиту общественных отношений по созданию, хранению, распространению, использованию и обеспечению сохранности и конфиденциальности информации. Действующий уголовный закон, к сожалению, не в полной мере отвечает реальным потребностям и теряет свой карательный потенциал. Уголовно-правовые нормы, направленные на противодействие преступлениям против информационной безопасности, де-факто разрознены, лишены связи друг с другом и не имеют системного характера (за исключением лишь гл. 28 УК РФ). Исходя из этого, трудно переоценить актуальность исследования проблемы уголовно-правовой охраны информационной безопасности.

Объектом диссертационного исследования выступают общественные отношения, возникающие в связи с совершением деяний, представляющих собой незаконное воздействие на информационные отношения, за что действующим законодательством РФ предусмотрена уголовная ответственность, в первую очередь с совершением преступлений в сфере компьютерной информации, а также формированием уголовно-правовой политики обеспечения информационной безопасности.

Предметом диссертационного исследования являются Конституция Российской Федерации, нормы международного права, уголовного и иных отраслей российского законодательства, подзаконные акты, связанные с регулированием вопросов обеспечения информационной безопасности, материалы правоприменительной практики и данные судебной статистики, имеющие отношение к изучаемой проблематике, уголовно-правовые нормы зарубежного законодательства, доктринальные разработки в соответствующей сфере.

Целью диссертационного исследования является формирование совокупности новых научных положений, дополняющих и развивающих теоретические основы уголовно-правового противодействия посягательствам на информационную безопасность, и разработка на этой основе путей совершенствования отдельных направлений уголовно-правовой политики в указанной сфере.

На достижение указанной цели направлено определение и решение круга следующих **задач**:

– рассмотреть существующие подходы к определению понятия и сущности информации и информационной безопасности в уголовно-правовой сфере, сформулировать на этой основе уголовно-правовое определение информации;

– выявить проблемы уголовно-правового обеспечения информационной безопасности в Российской Федерации;

– рассмотреть сквозь призму критического анализа современные

тенденции уголовно-правовой политики в сфере обеспечения информационной безопасности;

– дать общую характеристику современной информационной преступности и отдельных ее видов;

– уточнить специфику совершения деяния с использованием ИТС «Интернет» как квалифицирующего признака преступления;

– дать уголовно-правовую характеристику посягательств на безопасность компьютерной информации (ст. 272–274^2 УК РФ) с разработкой рекомендаций по их квалификации;

– сравнить международно-правовой и зарубежный опыт уголовно-правового противодействия преступлениям в сфере обеспечения информационной безопасности и установить перспективы его возможной имплементации в российское уголовное законодательство;

– разработать комплекс предложений, направленных на совершенствование действующего уголовного законодательства в сфере противодействия преступлениям против информационной безопасности.

Методологическую основу диссертационного исследования составляют общенаучные и частно-научные методы научного познания, такие как системный, формально-логический, структурно-функциональный, формально-юридический, сравнительно-правовой, исторический, социологический, статистический, аналогия. В основу исследования положен всеобщий диалектический метод познания.

Теоретическая основа диссертационного исследования представлена работами выдающихся отечественных правоведов, названных при характеристике степени разработанности темы, а также иных специалистов в области теории государства и права, уголовного права, криминологии, уголовно-процессуального права, обеспечения национальной безопасности, международного права и международного уголовного права. Кроме того, автором использованы труды специалистов в области информационного права, теории информации, обеспечения информационной безопасности.

Нормативная основа диссертационного исследования представлена Конституцией Российской Федерации, нормами международного и отечественного уголовного права, рядом федеральных конституционных законов, федеральных законов, указов Президента РФ, постановлений Правительства РФ, корреспондирующими нормами уголовного законодательства некоторых зарубежных стран – Белоруссии, Германии, Казахстана, Китая, Киргизии, Молдавии, США, Таджикистана, Туркменистана, Узбекистана.

Эмпирическая основа диссертационного исследования представлена статистическими данными, подготовленными ГИАЦ МВД РФ за период 2018–2023 гг.; определениями Конституционного Суда РФ, постановлениями Пленума Верховного Суда РФ, приговорами, вынесенными по уголовным делам о преступлениях, так или иначе связанных с негативным воздействием на информационную безопасность, Симоновского районного суда г. Москвы, Кировского районного суда г. Екатеринбурга, Судакского городского суда Республики Крым, Ленинского районного суда г. Краснодара, Бабушкинского районного суда г. Москвы, Свердловского и Кировского районных судов г. Красноярска, Саровского городского суда Нижегородской области и др. (всего изучено 207 приговоров), а также обобщенными результатами проведенного автором анкетирования 138 практических работников – 56 федеральных судей и 82 следователя.

Научная новизна диссертации состоит в том, что автором впервые с учетом дополнений, внесенных в УК РФ Федеральным законом от 14.07.2022 г. № 260-ФЗ[1], осуществлено комплексное исследование преступлений в сфере обеспечения информационной безопасности и защиты информации. Систематизация преступлений, в рамках которых информация рассматривается не только как предмет противоправного посягательства, но и может выступать признаком объективной стороны, привела к обоснованию нового подхода к классификации исследуемых деяний, формированию определения информации как предмета информационных отношений, выступающих объектом уголовно-правовой охраны.

Анализ современных тенденций уголовно-правовой политики противодействия преступлениям против информационной безопасности позволил сформировать вектор дальнейшей криминализации соответствующих деяний, выявить наиболее уязвимую и незащищенную сферу правового регулирования в исследуемой области, определить специфические особенности новых составов преступлений: экстерриториальность, широкий, практически неограниченный круг потерпевших, самораспространяемость и изменчивость, крайне высокий уровень латентности.

В диссертации обоснован вывод о том, что киберпространство приобретает все более осязаемые черты криминальной среды со своей контркультурой, отличительными, присущими только ему признаками. Очевидно, что в перспективе его возможно будет определять как новую форму реальности, а следовательно, – место совершения преступления.

Сравнительно-правовое исследование норм международного и зарубежного законодательства позволило объективно оценить уровень отечественной уголовного-правовой охраны соответствующих отношений, определить положения, представляющие интерес для возможной последующей имплементации в отечественное законодательство.

Результаты проведенного исследования позволили выработать комплекс как доктринальных положений, так и основанных на них законотворческих предложений, направленных на совершенствование норм действующего уголовного законодательства и правоприменительной практики в соответствующей их части.

Положения, выносимые на защиту:

1 В настоящее время в правовой науке отсутствует единое как уголовно-правое, так и обще-юридическое определение информации. При этом она рассматривается и как объект информационных отношений, и как объект передачи данных, поэтому требуется конкретизация соответствующего понятия, встречающегося в различных интерпретациях более чем в 18 кодексах российского права. В связи с этим предлагается следующее доктринальное определение *информации* – это подлежащие уголовно-правовой охране сведения конфиденциального характера, содержащие персональные данные или относящиеся к любой разновидности тайны, порядок допуска к которым, в том числе ознакомления с ними, их распространения, копирования, изменения, уничтожения, а также порядок и форма хранения подлежат императивному правовому регулированию, нарушение которых влечет уголовную ответственность.

2 Информационную безопасность в контексте уголовно-правовой теории

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14.07.2022 г. № 260-ФЗ // СПС «КонсультантПлюс». URL: https://www.consulta nt.ru/document/cons_doc_LAW_421797/ (дата обращения: 14.01.2023 г.).

необходимо рассматривать с нескольких позиций:

– защита сохранности и конфиденциальности данных, хранящихся как на электронных, так и на бумажных носителях, от преступных посягательств на них (похищение, уничтожение, изменение, незаконное распространение);

– защита сохранности и конфиденциальности информационно-коммуникационных систем, сайтов, информационных ресурсов и объектов критической информационной инфраструктуры;

– защита граждан и общества от распространения заведомо ложной информации, социально-опасной или недостоверной информации, направленной на причинение вреда личности, обществу, государству.

3 Общественные отношения, охраняемые уголовным законом в рамках уголовно-правовой политики в сфере обеспечения информационной безопасности, обладают следующими чертами и тенденциями:

– зарождение и развитие естественным путем единого информационного и медиапространства, позволяющего единовременно и практически без ограничений распространять информацию и сведения любого характера, в том числе осуществлять реализацию предметов, запрещенных к гражданскому обороту;

– формирование высокого уровня информационной культуры общества и как следствие – повсеместного внедрения электронных коммуникативных устройств и информационно-телекоммуникационных технологий;

– активное интегрирование информационной инфраструктуры в экономическую сферу общества, значительно влияющее на эффективность деятельности хозяйствующих субъектов, реализацию запрещенных товаров и услуг и т.д.;

– получение субъектами информационных отношений возможности оказания большего влияния на государственные, политические, экономические и управленческие процессы посредством использования информационных технологий (манипуляция, когнитивное воздействие, шантаж, дезинформация и размещение заведомо ложных или недостоверных, непроверенных новостей и т.д.);

– формирование у социума, представителей профессионального и научного сообщества запроса на модернизацию уголовного и уголовно-процессуального законодательства в сфере обеспечения информационной безопасности.

4 Объективный процесс всеобъемлющей цифровизации привел к новой социальной революции в общественных отношениях, в корне изменив порядок хранения, обмена, распространения информации во всех сферах жизнедеятельности, что повлекло трансформацию структурно-сущностных аспектов преступности, криминализацию ряда новых деяний, перечень, которых будет дополняться. Преступления, посягающие на информационную безопасность, обладают рядом специфических особенностей:

– экстерриториальность – большинство информационных преступлений совершается в виртуальной сфере с использованием электронных устройств, при этом виртуальная среда выступает в качестве ключевого признака такой преступности, так как позволяет преступнику анонимно и дистанционно осуществлять преступное деяние. Еще одной особенностью данного критерия выступает ощущение безнаказанности преступника, эфемерность которого напрямую зависит от уровня развития уголовного законодательства и профессионализма работников правоохранительных органов. Виртуальное деяние все очевиднее становится новой вехой в развитии преступности и требует от государственных органов соразмерной системной реакции;

– неограниченный или не устанавливаемый круг потерпевших – преступления, совершаемые с использованием информационно-коммуникационных технологий, нередко нацелены на неограниченное количество потерпевших, примером чего может служить массовая хакерская атака на банковский сектор, сайты и серверы государственных учреждений, массовые заведомо ложные сообщения об акте терроризма и т.д.;

– самораспространяемость – характерный для преступлений в сфере компьютерной информации признак, который выражается в самораспространении загружаемых в ИТС «Интернет» вирусов, способности программы к неограниченному повреждению напрямую не связанных между собой компьютерных систем, обусловливающих значительные трудности в оценке реального круга потерпевших, что ставит вопросы относительно оценки ущерба, места совершения преступления, направленности умысла и иных имеющих значение обстоятельств уголовно-правового характера;

– изменчивость – возросшая скорость научно-технического прогресса привела к тому, что каждая новая технология практически сразу находит применение в преступности – будь то алгоритмы искусственного интеллекта, теневой интернет, способы кодирования голоса, подделки отпечатков пальцев, программы взлома и т.д. В результате складывается динамически непрерывный процесс цифровой модернизации средств и способов совершения преступления, а также появляются де-факто новые, ранее не известные уголовному законодательству общественно опасные деяния, формально не подпадающие под существующие нормы Особенной части УК РФ;

– высокий уровень латентности преступлений против информационной безопасности – в настоящий момент практически нереально определить реальный ежегодный ущерб от такого рода преступлений, так как большинство из них остаются незарегистрированными и не выявленными, что во многом является следствием несовершенства законодательного (в том числе уголовного и уголовно-процессуального) и правоприменительного механизмов, а также бездействия самих потерпевших.

5 Преступления, именуемые как «информационные», «компьютерные», «киберпреступления» и т.п., предлагается объединить в общую группу с названием «*преступления против информационной безопасности*» и определить как запрещенные уголовным законом виновно совершаемые общественно опасные деяния, посягающие на безопасность, конфиденциальность информации, ее тайну и достоверность, конституционные права граждан в сфере информации, неприкосновенность и целостность информационно-коммуникационных систем, критических объектов информационной инфраструктуры.

Преступления против информационной безопасности предлагается классифицировать по следующим категориям (группам):

– преступления, посягающие на неприкосновенность информации, доступ к которой ограничен (государственная, личная, семейная, налоговая, коммерческая, следственная и иные виды тайны, конфиденциальная информация) (ст. 137, 138, 138^1, 275, 276, 283, 283^1, 283^2, 284 УК РФ);

– преступления, посягающие на право личности, общества, государства на объективную и достоверную информацию (ст. 200^6, 207^1, 207^2, 207^3, 217^2, 285^3, 287; 303, 306, 307, 308, 310, 311, 316 УК РФ);

– преступления, посягающие на безопасность и целостность информации (преступления в сфере электронной информации, создание вредоносных программ, взлом электронных баз данных граждан, аккаунтов в социальных сетях, незаконный оборот информации, в том числе полученной преступным

путем, уничтожение информации в любых ее формах) (ст. 272–274, 325, 326, 327, 327^1, 327^2 УК РФ);

– преступления, посягающие на безопасность и функционирование информационно-телекоммуникационных сетей, интернет-ресурсов, сайтов, баз данных, объектов критической информационной инфраструктуры (ст. 274^1–274^2 УК РФ);

– преступления, сопряженные с распространением социально опасной, ограниченной для обнародования или противоправной информации (ст. 205^2, 205^6, ч. 3 ст. 212, 242, 242^1, 284^3, 297, 298^1, 319, 336, 354, 354^1 УК РФ);

– преступления, совершаемые с применением информационно-коммуникационных технологий (ч. 2 ст. 110, ч. 3 ст. 110^1, ч. 2 ст. 128^1, п. «б» ч. 2 ст. 133, ч. 2 ст. 151^2, п «г» ч. 3 ст. 158, ст. 159^3, ст. 159^6, ч. 2 ст. 205^2, ч. 3 ст. 222, п. «в» ч. 3 и п. «в» ч. 5 ст. 222^1, п. «в» ч. 3 и п. «в» ч. 5 ст. 222^2, п. «б» ч. 2 ст. 228^1, п. «г» ч. 2 ст. 242^2, п. «г» ч. 2 ст. 245, ч. 2 ст. 274^2, ч. 2 ст. 280, ч. 2 ст. 280^1, п. «в» ч. 2 ст. 280^4 п. «в» ч. 2 и ч. 4 ст. 354^1 УК РФ).

6 Киберпространство и информационное пространство следует рассматривать как специфическую криминальную среду со своей, контркультурой, особенностями способов и средств совершения преступлений, влияющих на степень общественной опасности деяний, что в некоторых случаях уже фактически закреплено законодателем (нормы Особенной части УК РФ, где совершение деяния в ИТС «Интернет» выделено в качестве квалифицирующего признака).

Проанализировав их место в структуре состава преступления, в частности, в числе признаков, образующих объективную сторону, можно констатировать, что рассматривать нематериальное пространство как место совершения преступления пока преждевременно, так как оно сводится к конкретному серверу, компьютерному устройству или компьютерным сетям. Однако при этом следует уточнить территориальный принцип действия уголовного закона в пространстве путем определения соотношения киберпространства и информационного пространства, установив юрисдикцию государства над его национальным сегментом ИТС «Интернет» и распространив суверенитет за пределы материального мира, что позволит по-новому взглянуть на определение действия уголовного закона в пространстве.

При этом совершение преступления с использованием информационно-телекоммуникационных технологий, в том числе сети «Интернет», следует оценивать как обстоятельство, повышающее степень общественной опасности деяния (в том числе как обстоятельство, отягчающее наказание), вследствие упрощения процессов приготовления к нему, приискания способа и орудия совершения, последующего сокрытия следов содеянного.

7 Предлагается следующее доктринальное определение кибератаки с перспективой дальнейшей криминализации подобного деяния – это виновно совершаемые противоправные, общественно опасные деяния по массовому воздействию на компьютеры, компьютерные сети и системы, их блокированию, повреждению, уничтожению, получению удаленного доступа к ним в целях дестабилизации деятельности органов власти или международных организаций либо воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями.

8 Выявлена наметившаяся в международном уголовном праве тенденция регионализации международно-правовых актов, посвященных вопросам противодействия преступлениям против информационной безопасности, что приводит к изменению практики действия преступников – из стран-не подписантов против целей, объектов, находящихся в странах-подписантах, что

делает практически невозможным их установление и привлечение к уголовной ответственности.

Единственным способом эффективного уголовно-правового противодействия преступлениям в сфере информационной безопасности на международном уровне видится принятие всеобъемлющей конвенции, которая бы определила понятийно-категориальный аппарат, перечень соответствующих преступлений и их базовые признаки, понятие и критерии информационной войны, порядок координации и взаимодействия правоохранительных органов. При этом условие соблюдения цифрового и информационного суверенитета государств должно быть ключевым при выработке такого документа.

9 Сравнительно-правовое исследование положений зарубежного уголовного законодательства об ответственности за соответствующие преступления привело к выводу о перспективности заимствования опыта ФРГ по криминализации противоправной записи непубличных разговоров с последующей передачей ее третьим лицам, особенно если указанные действия повлекли за собой наступление тяжких последствий, а также распространения сведений (в отечественном уголовном законе – компьютерной информации), полученных преступным путем. Представляет интерес использование «мошенничества» как признака, характеризующего способ совершения преступления: получение доступа к охраняемой законом информации посредством обмана и злоупотребления доверием.

10 На основе рассмотрения содержания составов преступлений, предусмотренных ст. 272-274[2] УК РФ, вопросов их квалификации, соответствующих теоретических изысканий обоснован комплекс предложений по корректированию редакций ряда статей Особенной части УК РФ, содержащихся в гл. 28 УК РФ («Преступления в сфере компьютерной информации»), направленных на совершенствование уголовно-правового противодействия преступлениям против информационной безопасности.

Теоретическая значимость исследования выражается в том, что совокупность полученных новых научных знаний, касающихся проблем уголовно-правового обеспечения информационной безопасности, вносит определенный вклад в развитие доктрины уголовного права в соответствующей ее части.

Сформулированные автором идеи и положения могут послужить катализатором развития и прогресса уголовно-правовой науки, они подготавливают почву для дальнейших исследований в указанной области научного познания.

Практическая значимость исследования видится в том, что обоснованные в работе предложения нормотворческого характера, обоснованная автором правовая модель построения уголовно-правовых норм, содержащихся в гл. 28 УК РФ, могут быть использованы в процессе дальнейшего совершенствования уголовного законодательства, регламентирующего ответственность за посягательства на информационную безопасность, а разработанный автором терминологический аппарат и рекомендации по квалификации указанных преступлений – в правоприменительной деятельности, а также при формировании правовых позиций Верховного Суда РФ.

Достоверность результатов исследования обеспечена совокупностью использованных соискателем методов исследования, значительным объемом подвергнутого анализу национального, международного и зарубежного законодательства, широким кругом изученных научных трудов, репрезентативностью собранного и обобщенного эмпирического материала.

Апробация результатов исследования. Основные положения

диссертации отражены в 7 научных статьях, 4 из которых опубликованы в изданиях, рекомендованных ВАК Минобрнауки РФ.

Результаты исследования обсуждались на кафедре уголовного права и криминологии Кубанского государственного университета, на которой выполнена диссертация, представлялись на международных и всероссийских научно-практических конференциях: Всероссийская научно-практическая конференция с международным участием «Прогресс и преемственность в российском уголовном праве (к 95-летию УК РСФСР 1926 г. и 25-летию УК РФ 1996 г.)» (г. Краснодар, Кубанский государственный университет, 28-29.05.2021 г.); Международная научно-практическая конференция «Уголовно-правовые меры противодействия служебным, экономическим и иным преступлениям: современное состояние и пути оптимизации» (г. Ярославль, юридический факультет Ярославского государственного университета им. П.Г. Демидова, 30.09-1.10. 2022 г.); Международная научно-практическая конференция «Институциональные основы уголовного права РФ (к 70-летнему юбилею профессора В.П. Коняхина)» (г. Краснодар, Кубанский государственный университет, 01-02.02.2024 г.).

Структура диссертации определяется целью и задачами исследования. Работа включает введение, три главы, объединяющие двенадцать параграфов, заключение, список использованных источников и приложения.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во введении аргументирована актуальность изучаемой темы, определена степень её научной разработанности, поставлены цель и задачи диссертации, обоснована научная новизна, сформулированы основные положения, выносимые на защиту, описаны методологическая, нормативная, теоретическая и эмпирическая основы работы, теоретическая и практическая значимость, изложена информация о достоверности и апробации результатов исследования, а также о его структуре.

Первая глава «Обеспечение информационной безопасности: общетеоретические, уголовно-правовые и сравнительно-правовые аспекты» состоит из 4 параграфов. В первом параграфе *«Понятие и сущность информации и информационной безопасности»* проводится исторический анализ возникновения дефиниции «информация», появления и развития теории информации и системы информационной безопасности, их места и значения в федеральном, в том числе уголовном, законодательстве.

Соискателем выявлены проблемы установления пределов нормативно-правового определения информации, его взаимосвязи со смежными терминами, выделены основные виды, а также критерии информации и информационных отношений как объекта уголовно-правовой охраны: нормативность; достоверность; конфиденциальность; направленность; тайность.

На протяжении становления и развития общей теории информации в различных отраслях научного познания были сформированы многообразные подходы к пониманию информации, ее сущности и системно-структурным особенностям – технические, гуманитарные, философские, химико-биологические, юридические. Следствием этого явилось фактическое отсутствие единого универсального определения «информации» на момент проведения исследования.

В диссертации определено, что информационная безопасность – это не статичное явление, так как зачастую опасность представляет не только нарушение целостности и конфиденциальности любых данных – от государственной до личной и семейной тайны, но и последующее их распространение. Так, в частности, публикация каких-либо данных (о лице, о его

семье или близких) может быть использована для оказания давления на государственного или военного служащего при принятии им решения в рамках исполнения должностных или служебных обязанностей.

Проанализировав различные мнения и подходы к пониманию информации и информационной безопасности, соискатель резюмирует отсутствие доктринального единства научных позиций. В положении 1, выносимом на защиту, представлена авторская дефиниция информации.

Обеспечение информационной безопасности уголовно-правовыми средствами предполагает совершение следующих действий:

– оценку эффективности, соразмерности, целесообразности действующих норм уголовного закона, а также положений интерпретационных актов Пленума Верховного Суда РФ и в случае необходимости – криминализацию или декриминализацию тех или иных деяний в информационной сфере;

– организацию и взаимодействие уголовно-правовых, уголовно-процессуальных, криминалистических сфер, направленных на более эффективное осуществление уголовного судопроизводства;

– эффективное уголовно-правовое противодействие преступлениям против информационной безопасности;

– прогнозирование и оценку тенденций развития преступности против информационной безопасности с учетом достижений научно-технического прогресса.

Во втором параграфе *«Уголовно-правовое обеспечение информационной безопасности в Российской Федерации»* исследуются подходы к определению преступлений в сфере информационной безопасности, разграничению понятий «компьютерные преступления», «преступления в сфере информационной безопасности», «преступления против компьютерной информации», «It-преступления».

Соискатель приходит к выводу, что УК РФ в действующей редакции выделяет три группы компьютерных преступлений:

– преступления в сфере компьютерной информации, (непосредственно компьютерные преступления – гл. 28 УК РФ);

– «общеуголовные» преступления, для которых использование компьютерной техники или оборудования указано способом их совершения (например, ч. 3 ст. 141, ст. 159^6 УК РФ и др.);

– преступления общеуголовного характера, совершаемые с использованием виртуальных сетей, в том числе ИТС «Интернет» (ст. 110, 110^1, 110^2, 228^1, 282 УК РФ и др.).

Очевидно, что далеко не все указанные деяния следует относить к преступлениям против информационной безопасности в силу содержания их объекта. Некоторые компьютерные преступления возможно рассматривать как вид преступлений, посягающих на информационные отношения.

Помимо преступлений, сопряженных непосредственно с компьютерной информацией, УК РФ обеспечивает охрану информационных прав граждан посредством установления ответственности за оборот социально опасной информации различной направленности. В некоторые случаях она может выступать в качестве предмета преступления, а ее распространение, выраженное в публичном призыве, дискредитации или пропаганде, характеристикой его объективной стороны.

Информационное пространство как новая реальность в философском смысле и виртуальное пространство в техническом все чаще становятся местом совершения преступлений, а информация или слово – предметом или средством посягательства.

Преступления против информационной безопасности предложено классифицировать по определенным категориям, что отражено в положении 5, вынесенном на защиту.

Третий параграф *«Обеспечение информационной безопасности в международном уголовном праве»* посвящен анализу проблем международно-правового ее обеспечения.

В работе выявлено отсутствие унифицированной системы международного уголовно-правового обеспечения информационной безопасности, отмечена тенденция на его сегментирование и регионализацию, что продиктовано политико-экономическими причинами поляризации современных международных отношений.

Автором обращено внимание, что в ряде международных актов легализованы принципиально новые определения, не принятые на всеобщем уровне, но используемые и внедряемые на регионально-блоковом, например в Соглашении между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г., – «информационная война», «информационное пространство», «киберпространство» и т.д.

В диссертации указано на наличие запроса на принятие всеобъемлющей Хартии информационных прав с уклоном на цифровой аспект, а также специфику проведения информационных операций. Информация перестает быть исключительно предметом уголовно-правовой охраны, трансформируясь, она становится средством совершения преступления, а информационное/киберпространство отчетливо приобретает черты места его осуществления.

Таким образом, в настоящее время на международном уровне происходит активное формирование будущей архитектуры правового обеспечения информационной безопасности. Уголовно-правовые аспекты в данном случае играют ключевую роль, так как количество информационных операций и кибератак растет в геометрической прогрессии, они становятся более разнонаправленными, и их классификация усложняется. Отсутствие единого международного договора, определяющего кибератаки, механизм уголовно-правовой борьбы с ними, позволяет их использовать в качестве инструмента политического воздействия.

Четвертый параграф *«Обеспечение информационной безопасности в зарубежном уголовном праве*» посвящен анализу уголовно-правовой практики противодействия преступлениям, направленным против информационной безопасности, на примере законов ряда зарубежных государств (КНР, США, Германия, Великобритания и др.).

Так, УК Китая рассматривает виртуальное пространство (киберпространство) как правовую категорию, обладающую всеми чертами места совершения преступления. В его рамках возможно совершение публичного оскорбления, вторжения в государственные информационные системы, их последующее разрушение.

Соискателем отмечается, что в американской уголовно-правовой доктрине большое внимание обращено на вопросы противодействия кибертерроризму, отмечается широкий плюрализм мнений относительно его идентификации, в законе самостоятельно криминализируется раскрытие конфиденциальной информации как особого критерия информационной преступности. На основе анализа отдельных законодательных актов США соискатель выделяет некоторые основные направления уголовно-правового обеспечения информационной

безопасности в США, целостности, конфиденциальности, гарантии подлинности соответствующих данных.

Изучив особенности уголовно-правовой охраны информации в ФРГ, соискатель отмечает деяния, которые в УК РФ не криминализованы, – перехват информации, в том числе компьютерной, сторонним пользователем, передача информации, к которой доступ получен неправомерным путем третьими лицами, незаконная запись голоса человека и т.д. Указано, что перспектива рецепции указанных норм в УК РФ имеет достаточно серьезные основания.

В уголовном законодательстве Франции и Великобритании интерес вызывает детальное регулирование ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры, незаконный ввоз специального технического оборудования, при помощи которого возможно осуществление воздействия на объекты КИИ.

Подытоживая анализ в названном разделе диссертации, соискатель заключает, что у большинства государств сформирована серьезная уголовно-правовая база противодействия преступлениям в сфере информационной безопасности; в большинстве случаев криминализированы деяния, связанные с неправомерным доступом к охраняемой законом информации, неправомерным воздействием на объекты критической информационной инфраструктуры, информации сети и т.д. Вместе с тем мировой масштаб проблемы требует консолидированных усилий в соответствующей сфере и принятия на уровне ООН международной Всеобъемлющей конвенции по международной информационной безопасности. Тенденция регионализации международных актов по противодействию указанным преступлениям приведет к тому, что злоумышленники будут действовать из стран не подписантов против целей/объектов, находящихся в странах-подписантах.

Вторая глава «Современная уголовно-правовая политика России в сфере обеспечения информационной безопасности» состоит из трех параграфов.

В *первом параграфе* «Тенденции уголовно-правовой политики в сфере обеспечения информационной безопасности» соискать анализирует развитие процесса уголовно-правовой регламентации охраны информационных отношений, криминализации соответствующих деяний, уголовно-правовое регулирование киберпространства, специфику преступлений, направленных против информационной безопасности.

Автор приходит к выводу, что анализ современного уровня уголовно-правовой охраны информационных отношений позволяет констатировать наличие тенденции модернизации уголовного закона в связи с появлением качественно новых общественных отношений и их информатизацией, формированием системы защиты информации, построением информационно-коммуникационной инфраструктуры. Законодатель в последние 10–15 лет взял уверенный курс на криминализацию деяний, посягающих на отношения в сфере обеспечения информационной безопасности, что выражается в появлении новых 14 составов преступлений, модернизации 17, уже существующих, и отсутствии тенденции к декриминализации соответствующих деяний. Вместе с тем наблюдается разрозненность норм, направленных на охрану информационных отношений, содержащихся в Особенной части УК РФ, что препятствует, в том числе, эффективному процессу правоприменения. При этом очевидна необходимость криминализации таких деяний, как неправомерное собирание и хранение персональных данных физических лиц, незаконный оборот персональных данных физических лиц. В ближайшем будущем возникнет необходимость уголовно-правовой оценки деятельности по реализации программ, созданных в рамках технологий искусственного интеллекта.

Соискатель полагает, что стремительное развитие информационно-коммуникационных технологий привело к формированию новых социально-правовых явлений – киберпространства и информационного пространства. Однако анализ их статуса в системе признаков состава преступления, характеризующих деяние, привел к выводу, что определять нематериальное пространство как место совершения посягательства пока преждевременно, так как оно сводится к конкретному серверу, компьютерному устройству или компьютерным сетям. Киберпространство и информационное пространство следует определять как криминальную среду со своей спецификой, контркультурой, особенностями способов и средств совершения преступлений, влияющую на степень общественной опасности, что в некоторых случаях законодателем уже учтено (нормы Особенной части УК РФ, где совершение деяния в ИТС «Интернет» выделено в качестве квалифицирующего признака).

Во *втором параграфе «*Общая характеристика современной информационной преступности и отдельных ее видов» рассматривается современная киберпреступность, ее специфика и особенности. В итоге проведенного анализа соискатель предлагает авторское доктринальное определение кибератаки, отраженное в положении 7, вынесенном на защиту.

Соискатель, кроме того, приходит к выводу, что в теории уголовного права должны найти закрепление определение и характеристика информационной войны, так как на международном уровне она уже получила свое официальное нормативное определение. Для уголовно-правового противодействия информационным войнам требуется установление критериев противоправности соответствующих деяний, обоснование уровня их общественной опасности и последствий.

Необходимо рассматривать информационную безопасность не только в контексте преступлений в сфере компьютерной информации, но и тех уголовно-правовых деликтов, которые связаны с распространением информации различного свойства и содержания как способом их совершения.

В *третьем параграфе* «Совершение преступлений с использованием ИТС «Интернет» как квалифицирующий признак деяния» автор отмечает, что за последнее десятилетие в закон введен ряд новых составов, отличительной чертой которых является наличие следующего квалифицирующего признака – «использование информационно-телекоммуникационных сетей (включая ИТС «Интернет»). Если дифференцировать процесс закрепления названного обстоятельства, то, исходя из объекта соответствующих деяний, его можно представить следующим образом:

– преступления против жизни и здоровья (п. «д» ч. 2 ст. 110, ст. 110^1, 110^2 УК РФ);

– преступления против свободы, чести и достоинства личности (ч. 2 ст. 128^1 УК РФ);

– преступления против половой неприкосновенности и половой свободы личности (п. «б» ч. 3 ст. 133 УК РФ);

– преступления против семьи и несовершеннолетних (п. «в» ч. 2 ст. 151^2 УК РФ);

– преступления против общественной безопасности (ч. 2 ст. 205^2, п. «в» ч. 3, п. «в» ч. 5 ст. 222, п. «в» ч. 3, п. «в» ч. 5 ст. 222^1, п. «в» ч. 3, п. «в» ч. 5 ст. 222^2 УК РФ);

– преступления против здоровья населения и общественной нравственности (п. «б» ч. 2 ст. 228^1, п. «д» ч 2 ст. 230, ч 1^1 ст. 238^1, п. «б» ч. 3 ст. 242, п. «г» ч. 2 ст. 242^1, «г» ч. 2 ст. 242^2, п. «г» ч. 2 ст. 245 УК РФ);

– экологические преступления (п. «б» ч. 2 ст. 258^1 УК РФ);

– преступления против основ конституционного строя и безопасности государства (ч. 2 ст. 280, ч. 2 ст. 280^1, п. «в» ч. 2 ст. 280^4, ст. 282 УК РФ);

– преступления против мира и безопасности человечества (п. «в» ч. 2, ч. 4 ст. 354^1 УК РФ).

В 2023 г. сложилась судебная практика квалификации использования ИТС «Интернет» для подготовки к совершению противоправного деяния, координации действий исполнителя с иными соучастниками. Так, Верховный Суд РФ установил, что переписка в мессенджерах (социальных сетях) относительно подготовки и дальнейшей реализации преступного умысла должна оцениваться с учетом квалифицирующего признака – с использованием ИТС «Интернет». Таким образом, любое, по сути, преступление, при подготовке или совершении которого использовались ресурсы или возможности ИТС «Интернет», должно квалифицироваться с учетом данного признака. Тем не менее, не все необходимые статьи УК РФ содержат указание на такое обстоятельство, поэтому соискатель приходит к выводу о целесообразности расширения перечня обстоятельств, отягчающих наказание, за счет его включения.

Третья глава «Посягательства на безопасность компьютерной информации в Российской Федерации: уголовно-правовая характеристика (ст. 272–274^2 УК РФ)» состоит из пяти параграфов.

Первый параграф *«Неправомерный доступ к компьютерной информации»* посвящен рассмотрению содержания состава и проблем квалификации преступления, указанного в ст. 272 УК РФ.

Выявив достоинства и недостатки конструкции состава названного преступления, осуществив краткий обзор судебной практики, анализ теоретических позиций ученых, автор отмечает, что согласно ст. 1 УК РФ, уголовное законодательство РФ состоит исключительно из уголовного кодекса. Вместе с тем сущностные характеристики общественно опасных последствий, напрямую влияющих на квалификацию, строгость и вид наказания за совершение преступления, предусмотренного ст. 272 УК РФ, содержатся в постановлении Пленума Верховного Суда РФ, что вряд ли оправдано. В результате рассмотрения предложена скорректированная редакция ст. 272 УК РФ:

*«**Статья 272. Неправомерный доступ к компьютерной информации***

1 Осуществление неправомерного доступа к охраняемой законом компьютерной информации и последующее ознакомление с ней, –

наказывается…

2 То же деяние:

а) совершенное из корыстной заинтересованности;

б) повлекшее причинение крупного ущерба;

в) совершенное группой лиц по предварительному сговору;

г) совершенное лицом с использованием своего служебного положения;

д) повлекшее модификацию, уничтожение, блокирование или копирование информации, –

наказывается…

3 Деяния, предусмотренные частями первой или второй настоящей статьи, совершаемые с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные, –

наказываются…

4 Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или совершены организованной группой, –

наказываются...

Примечания.

1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи, относящиеся к персональным данным, личной, семейной или иной форме тайны, инсайдерской информации.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.

3. Под уничтожением компьютерной информации следует понимать ее полное фактическое удаление с носителя, сервера, баз данных без возможности последующего восстановления.

4. Под повреждением компьютерной информации следует понимать такое частичное или полное удаление её с носителя, сервера, баз данных, которое впоследствии можно восстановить или устранить.

5. Под блокированием компьютерной информации признается такое воздействие на нее, средство доступа, источник хранения (компьютер, сервер или иное электронное устройство), которое приводит к невозможности использования или ознакомления с информацией в течение производного количества времени.

6. Под модификацией компьютерной информации понимается внесение в нее изменений, повлекших изменение ее свойств, целостности или достоверности.

7. Под копированием компьютерной информации понимается перенос/создание копии информации, к которой получен неправомерный доступ, на другой электронный носитель, либо воспроизведение ее в материальной форме при условиях сохранения ее в неизменной первоначальной форме».

Во втором параграфе *«Создание, распространение и использование вредоносных компьютерных программ»* охарактеризовано содержание состава и вопросы квалификации деяния, криминализованного в ст. 273 УК РФ, а также соответствующие теоретические изыскания, касающиеся данного преступления. В результате предложено скорректировать действующую редакцию нормы:

«Статья 273. Создание, использование, распространение и приобретение вредоносной компьютерной программы или иной компьютерной информации

1 Создание, использование, распространение или приобретение вредоносной компьютерной программы или иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, повреждения, блокирования, модификации, копирования компьютерной информации, а равно ознакомление с ней, осуществление слежения за компьютерным устройством, ограничение доступа к информационно-телекоммуникационным ресурсам в сети «Интернет», нейтрализация средств защиты компьютерной информации –

наказываются…

2 То же деяние:

а) совершенное из корыстной заинтересованности;

б) повлекшее причинение крупного ущерба;

в) совершенное группой лиц по предварительному сговору;

г) совершенное лицом с использованием своего служебного положения,

– наказывается…

3 Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные с трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные, –

наказываются…

4 Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или совершены организованной группой, –

наказываются…».

Здесь же представлена авторская дефиниция вредоносной компьютерной программы – это программа, созданная на языке программирования и заведомо предназначенная для неправомерного доступа к компьютерным устройствам и воздействия на них в целях уничтожения, повреждения, модификации, копирования компьютерной информации, ознакомления с ней, осуществления слежения за компьютерным устройством, ограничения доступа к информационно-телекоммуникационным ресурсам в сети «Интернет», нейтрализации средств защиты компьютерной информации.

В третьем параграфе *«Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»* отмечается, что решение об установлении уголовной ответственности за данное преступление является дискуссионным. Связано это, в первую очередь, с тем, что ст. 274 УК РФ применяет в судебно-следственной практике крайне редко.

Соискателем выделяется несколько моментов, связанных с применением анализируемой нормы. Во-первых, как показала практика, к правилам относятся не только нормы, предусмотренные федеральным законодательством, в том числе ГОСТы и СанПиНы, но и внутренние нормы и правила отдельных предприятий, особенно связанных с обеспечением различных видов тайн. Во-вторых, лицо, совершающее преступление, нередко нарушает соответствующие правила из корыстных или иных личных побуждений, что не нашло отражения в законе. В-третьих, предусмотренное законом наказание в виде лишения свободы на срок до 2 лет по ч. 1 и до 5 лет по ч. 2 статьи крайне гуманно, исходя из тяжести последствий, которые могут наступить в случае совершения преступления.

Автором предложены направления коррекции редакции ст. 274 УК РФ:

«Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

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

наказывается…

2 Деяние, предусмотренное частью первой настоящей статьи:

а) повлекшее прекращение работы предприятия на срок более суток;

б) повлекшее получение доступа к сведениям, составляющим различные виды тайны;

в) повлекшее причинение тяжкого вреда здоровью по неосторожности;

г) совершенное из корыстной или иной личной заинтересованности;

д) совершенное группой лиц по предварительному сговору

е) совершенное с целью скрыть другое преступление, –

наказывается…

3 Деяние, предусмотренное частью первой или второй настоящей статьи:

а) повлекшее прекращение работы предприятия на срок более недели;

б) повлекшее получение доступа к сведениям, составляющим государственную тайну;

в) повлекшее причинение по неосторожности смерти человека;

г) совершенное организованной группой, –

наказывается…».

Четвертый параграф *«Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»* посвящен уголовно-правовому рассмотрению одноименного состава преступления (ст. 274^1 УК РФ) и проблемам квалификации деяния.

Развитие информационных технологий, средств связи, коммуникаций, «Интернета» стало причиной повсеместного процесса цифровизации. Крупные компании, предприятия, организации и прочие объекты инфраструктуры теперь обладают собственными облачными хранилищами и серверами для хранения, обработки, передачи компьютерной информации. Данная тенденция имеет ряд как положительных, так и отрицательных сторон. С одной стороны, это, безусловно, развитие, ускорение общественной жизни, рост ее качества, доступности медицины, электроэнергии, транспорта, скорости Интернета и т.д. С другой, рост зависимости общества и государства от информационных систем, отключение которых способно на продолжительный промежуток времени парализовать ставшие уже естественными процессы жизнедеятельности.

Осложнение внешнеполитической обстановки неизменно влечет рост информационных атак или кибератак на объекты критической информационной инфраструктуры (далее – КИИ) РФ. Именно существенное увеличение числа подобных преступных по своей природе деяний стало причиной включения в 2017 г. в гл. 28 УК РФ статьи 274^1.

Автор замечает, что конструирование в ч. 2 статьи материального состава исключает ответственность за неправомерный доступ к компьютерной информации объекта КИИ, не повлекший указанных в законе последствий. Например, в ситуации, когда лицо, реализуя преступный умысел, направленный на исследование и изучение системы функционирования и структуры объекта КИИ, из корыстной или иной личной заинтересованности осуществляет неправомерный доступ к охраняемой законом компьютерной информации на объекте КИИ, однако не наносит вред самой системе, а лишь изучает ее, в том числе получая, например, сведения, составляющие государственную тайну, или осуществляет удаленное слежение за ней.

Соискателем разработана обновленная редакция ст. 274^1 УК РФ:

«Статья 274^1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

1 Создание, приобретение, распространение и (или) использование компьютерной программы либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для ознакомления, уничтожения, блокирования, повреждения, модификации, копирования, отслеживания информации, содержащейся в ней, или нейтрализации средств защиты указанной информации, –

наказываются…

2 Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных

программ с целью ознакомления, уничтожения, блокирования, повреждения, модификации, копирования, отслеживания информации, содержащейся в ней, –

наказывается….

3 Деяния, предусмотренные частью первой настоящей статьи:

а) повлекшие прекращение работы предприятия на срок более суток;

б) повлекшие получение доступа к сведениям, составляющим различные виды тайны;

в) повлекшие причинение тяжкого вреда здоровью по неосторожности;

г) совершенные из корыстной или иной личной заинтересованности;

д) совершенные группой лиц по предварительному сговору

е) совершенные с целью скрыть другое преступление, –

наказываются…

4 Деяния, предусмотренные частью первой или второй настоящей статьи:

а) повлекшие прекращение работы предприятия на срок более недели;

б) повлекшие получение доступа к сведениям, составляющим государственную тайну;

в) повлекшие причинение по неосторожности смерти человека;

г) совершенные организованной группой, –

наказывается…».

В пятом параграфе *«Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования»* представлен анализ состава этого преступления и проблем его квалификации (ст. 274^2 УК РФ).

Автор обращает внимание на сложности в определении содержания состава преступления вследствие бланкетности предусматривающих его норм, отсутствие правоприменительной практики из-за сравнительно небольшого периода времени, прошедшего с момента криминализации данного деяния. В силу этого обстоятельства практически невозможно оценить перспективы «работы» названной статьи, а также выявить проблемы, которые могут возникнуть в процессе правоприменения.

Подводя итоги рассмотрения, осуществленного в рамках третьей главы, соискатель делает следующие выводы:

– нормы, закрепленные в гл. 28 УК РФ, являются востребованными, так как с каждым годом число зарегистрированных преступлений, ими предусмотренных, возрастает;

– вместе с тем конструкция диспозиций почти всех этих норм характеризуется наличием некоторых неточностей и неопределенностей, которые критикуются представителями уголовно-правовой науки и требуют устранения;

– представляется закономерным в перспективе преступления против информационной безопасности выделить в самостоятельный раздел, но данное предложение требует дальнейшего изучения и обсуждения.

В **заключении** подведены итоги исследования, сформулированы основные авторские выводы и предложения.

В приложении 1 к диссертации представлен разработанный соискателем комплекс предложений по корректированию редакций ст. 272–274^1 УК РФ гл. 28 УК РФ, направленных на совершенствование уголовно-правового противодействия преступлениям против информационной безопасности.

Приложение 2 содержит опросный лист и обобщенные результаты анкетирования 138 респондентов – 82 следователя и 56 судей – по различным аспектам исследуемой темы.

Основные положения диссертации нашли отражение в следующих публикациях автора *(общий объем – 2,85 п.л., авторский вклад – 2,85 п.л.):*

Статьи в рецензируемых изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования РФ для опубликования результатов диссертационных исследований:

1. Лихачев, Н.А. Перспективы совершенствования уголовно-правовых норм, предусматривающих ответственность за создание, использование и распространение вредоносных компьютерных программ / Н.А. Лихачев // Теория и практика общественного развития. – 2023. – № 5. – С. 176–180 (0,5 п.л.).

2. Лихачев, Н.А. Неправомерный доступ к компьютерной информации: направления оптимизации состава / Н.А. Лихачев // Гуманитарные, социально-экономические т общественные науки. – 2023. – № 4. – С. 153–157 (0,45 п.л.).

3. Лихачев, Н.А. Проблема понимания определения и сущности компьютерной преступности в контексте обеспечения информационной безопасности / Н.А. Лихачев // Международный научно-исследовательский журнал. – 2023. – № 6. – С. 438–443 (0,4 п.л.).

4. Лихачев, Н.А. Нематериальное пространство как новая форма места совершения преступления: доктринальный аспект / Н.А. Лихачев // Юридические исследования. – 2024. – № 4. – С. 1–8 (0,5 п.л.).

Научные статьи, опубликованные в иных изданиях:

5 Лихачев, Н.А. Современная уголовная политика Российской Федерации в сфере обеспечения информационной безопасности / Н.А. Лихачев // Прогресс и преемственность в российском уголовном праве (к 95-летию УК РСФСР 1926 г. и 25-летию УК РФ 1996 г.): материалы Всероссийской научно-практической конференции с международным участием (г. Краснодар, 28-29.05.2021 г.). – Краснодар: Кубанский государственный университет, 2021. – С. 637–642 (0,4 п.л.).

6 Лихачев, Н.А. Уголовно-правовые меры противодействия преступлениям, связанным с посягательствами на персональные данные граждан / Н.А. Лихачев // Уголовно-правовые меры противодействия служебным, экономическим и иным преступлениям: современное состояние и пути оптимизации: материалы Международной научно-практической конференции (г. Ярославль, 30.09-1.10.2022 г.). – Ярославль: Ярославский государственный университет им. П.Г. Демидова, 2022. – С. 83–87 (0,2 п.л.).

7 Лихачев, Н.А. Проблемы квалификации преступлений экстремистской направленности / Н.А. Лихачев // Институциональные основы уголовного права РФ (к 70-летнему юбилею профессора В.П. Коняхина): материалы Международной научно-практической конференции (г. Краснодар, 01.-02.02.2024 г.). – Краснодар: Кубанский государственный университет, 2024. – С. 527–530 (0,4 п.л.).

Л и х а ч е в Никита Александрович

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ ПРЕСТУПЛЕНИЯМ В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ЗАКОНОДАТЕЛЬНЫЙ, ПРАВОПРИМЕНИТЕЛЬНЫЙ И ДОКТРИНАЛЬНЫЙ АСПЕКТЫ

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Подписано в печать 24.04.2024. Формат 60Х84 1/16
Печать цифровая. Объем 1,5 п.л. Тираж 150 экз. Заказ № ____

Тираж отпечатан с оригинал-макета заказчика
в типографии ООО «Просвещение-Юг»
350080, г. Краснодар, ул. Бородинская, 160/5