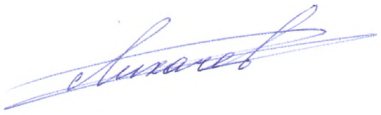
Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

На правах рукописи



ЛИХАЧЕВ НИКИТА АЛЕКСАНДРОВИЧ

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

5.1.4. Уголовно-правовые науки
(юридические науки)

Диссертация

на соискание ученой степени

кандидата юридических наук

Научный руководитель:
заслуженный юрист РФ,
заслуженный работник высшей школы РФ,
доктор юридических наук, профессор
Прохоров Л.А.

Краснодар
2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

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

[1] Статистика и аналитика МВД России. URL: https://xn--b1aew.xn--p1ai/reports/item/16053092/ (дата обращения: 14.02.2024 г.). Здесь и далее показатели сформированы в соответствии с Перечнем № 25, введенным в действие указанием Генеральной прокуратуры Российской Федерации и Министерства внутренних дел Российской Федерации «О введении в действие перечней статей Уголовного кодекса Российской Федерации, используемых при формировании статистической отчетности» от 30 июня 2022 года № 361/11/1.

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

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[1]. Как отмечается в отчетах МВД РФ, их профилактика по-прежнему остается одной из важнейших задач органов внутренних дел[2].

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[3]. 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[4]).

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

---

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

[2] 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.).

[3] 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.).

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

«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].

---

[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

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 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

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.).

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, упомянутых 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.

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 – по тем или иным проблемам исследования.

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

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14.07.2022 г.

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

№ 260-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_421797/. (дата обращения: 14.01.2023 г.).

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, однако требует конкретизации 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 ознакомление с ними, их распространение, копирование, изменение, уничтожение, а также порядок и форма хранения, подлежит императивному правовому регулированию, нарушение которого влечет уголовную ответственность.

2 Информационную безопасность в контексте уголовно-правовой теории 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 объектов, 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 общества, 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 уголовно-правового 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 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 (представлен в приложении 1 к диссертации).

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.

1 Обеспечение информационной безопасности: общетеоретические, уголовно-правовые и сравнительно-правовые аспекты

1.1 Понятие и сущность информации и информационной безопасности

В XXI в. информация окончательно приобрела черты ключевых стратегически ресурсов, за обладание которыми ведут между собой борьбу транснациональные корпорации, международные организации и государства. Стремительное развитие научно-технического прогресса ускорило процессы обмена данными, в результате чего объемы потребления информации в обществе качественно возросли. Всеобъемлющий процесс цифровизации привел к формированию глобального киберпространства, содержащего сведения, относящиеся практически ко всем формам тайны, – от личной до государственной.

Понятие «информация» относится к одному из самых общеупотребимых и трудноопределимых терминов. С одной стороны, он интуитивно понятен каждому, но, с другой, его фактическое отражение в науке весьма затруднительно в связи с проблемами определения сущности, критериев и признаков. Информация является свойством любого языка и речи, продуктом мыслительного процесса человека, отражением объектов материальной действительности и нематериального мира.

Слово «информация» возникло в русской речи в эпоху Петра I Великого во время процесса реформирования языка, оно было заимствовано из польского – «informacja». В польский язык, в свою очередь, это слово пришло из латинского – «informatio», что переводится как «представление», «разъяснение», «изложение»[1]. Выдвигается также гипотеза, предполагающая,

[1] Семёнов А.В. Этимологический словарь русского языка. Русский язык от А до Я. М.: ЮНВЕС, 2003. С. 478.

что первоначальным источником было другое латинское слово – «informare» (доводить до сведения»)[1].

С течением времени процессы создания, хранения и передачи информации менялись, становясь более сложными и разнообразными, – от примитивного языка жестов до современных электронных технологий и «больших данных». Понимание термина, его сущностное знание претерпевало трансформацию и становилось многоаспектным (техническим, юридическим, экономическим, философским, и т.д.). На сегодняшний день встречается несколько десятков его толкований. В первую очередь это связано с тем, что слово «информация» широко используется не только как наукоемкий термин, но и как элемент повседневно-бытовой коммуникации в обществе. К информации относят сведения, данные, новости, сигналы, символы, материю и иные объекты или предметы, способные отражать, воспринимать или передавать материальную действительность. Информация способна оказывать влияние как на отдельно взятого человека, так и на целые социальные группы и общности людей в процессе ее интерпретации сквозь призму знаний и накопленного опыта.

Толковый словарь С. И. Ожегова определяет слово «информация» в двух значениях: как «сведения об окружающем мире и протекающих в нем процессах, воспринимаемых человеком или специальными устройствами» (специальный технический подход из теории информации), и как «сообщения, осведомляющие о положении дел или состоянии чего-либо»[2].

Современный толковый словарь русского языка аналогично определяет значение слова «информация», дополняя его следующим синонимичным значением – «информирование о положении дел в какой-либо области

[1] Волков Ю.В. Информационное право. Информация как правовая категория: учеб. пос. для вузов. 2-е изд. М.: Юрайт, 2023. С. 23.

[2] Ожегов С.И. Словарь русского языка: ок. 57000 слов / под ред. Н.Ю. Шведовой. 13-е изд., испр. М.: Просвещение, 1981. С. 224.

и о каких-либо событиях»[1].

Возникновение теории информации, ее профильное осмысление связано с развитием математики и философии на рубеже 20-30-х г. XX в. В 1928 г. Р. Хартли разработал формулу, позволяющую определить количество информации, то есть с выделением ее количественного признака или критерия. Суть заключается в том, что данный показатель должен согласовываться с интуитивным представлением субъекта о содержании в конкретном сообщении, шифре, тексте – источнике. Иначе говоря, чем больше объем у условного объекта познания, тем существеннее его информационная составляющая. Так, Р. Хартли связал понятие информации со сферой коммуникации, что во многом определило его дальнейшее развитие.

Его идеи были развиты К. Шенноном в работе «Математическая теория связи»: сообщения, уменьшающие неопределенность у получателя информации[2]. Таким образом, показатели прироста информации, ее значимость прямо пропорциональна уменьшению неопределенности по какому-либо вопросу. Именно К. Шеннон предложил действующую наименьшую единицу измерения цифровой/компьютерной информации – «бит». Он внес существенный вклад в развитие кибернетики. Н. Винер рассматривал информацию как обозначение содержания, полученного от внешнего мира в процессе приспособления к нему[3].

Таким образом, со временем информация как метафизическое явление стала обретать качественные, количественные и иные критерии. Чаще все ее отождествляют с энтропией в теории информации. В юриспруденцию это понятие было рецепировано из естественных наук (преимущественно из математики и физики). Однако на данный момент исчерпывающего и универсального определения информации не существует.

---

[1] Кузнецов С.А. Современный толковый словарь русского языка. М.: Норинт, 2004. С. 248.

[2] Шеннон К. Работы по теории информации и кибернетике. М.: Иностранная литература, 1963. С. 333-369.

[3] Винер Н. Кибернетика и общество. М.: Иностранная литература, 1958. С. 201.

Тем не менее, естественно-научное и юридическое определения информации не следует полностью отождествлять, так как правовые, математические, физические и иные категории преследуют разные цели, имеют отличный предмет и сферу научного познания. Важным является вопрос определения информации как объекта (познаваемые субъектом сведения) или действия (меры, умаляющие неопределенность в познании какого-либо вопроса).

На сегодняшний день информация является особым объектом как в отечественном, так и в зарубежном праве. Развитие информационной и цифровой отраслей за последние десятилетия существенным образом расширило ее устоявшееся понимание. Внедрение цифровой валюты и прав[1] изменило подходы к информации, подлежащей, в том числе, и уголовно-правовой охране. В последние десятилетия она приобрела свойства основополагающего фактора на уровне материи и энергии и рассматривается как новый вид капитала экономического, культурного и политического характера, подверженного различным формам криминального воздействия.

Российский законодатель официальное понимание информации отразил в Федеральном законе от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Согласно ст. 2 Закона информация – это сведения (сообщения или данные) независимо от формы их представления[2]. Отметим, что данный подход является максимально широким и размытым, что затрудняет определение предмета его содержания.

Это была не единственная попытка законодателя детерминировать дефиницию. Так, впервые в ФЗ от 20.02.1995 г. № 24-ФЗ «Об информации, информатизации и защите информации» в ст. 1 она определялась

[1] Гражданский кодекс Российской Федерации (ГК РФ) №51-ФЗ (ред. от 11 марта 2024 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_5142/ (дата обращения: 14.03.2024 г.).

[2] Об информации, информационных технологиях и о защите информации: Федеральный Закон от 27 июля 2006 г. № 149-ФЗ (ред. от 12 декабря 2023 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/? ysclid=lfs4b5a1bp112283080. (дата обращения: 14.01.2023 г.).

как «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления»[1].

Сопоставительный анализ текста двух федеральных законов показывает, что законодатель пошел по пути упрощения формулировки, что, с одной стороны, делает ее более доступной для понимания в обыденном (интуитивном) смысле, а с другой, способствует возникновению неопределенности с формально-юридической точки зрения. В результате термин приобретает универсальный характер, определяя, по сути, любой источник и форму передачи информации. Однако в данных формулировках не решается проблема определения первичности – объекта или действия.

В юридической науке и нормах российского законодательства встречаются иные понятия, прямо или косвенно относящиеся к информации. Выделим некоторые из них: «цифровая информация», «электронная информация», «компьютерная информация», «виртуальная информация», а также смежные понятия – «персональные данные», «личные данные», «дезинформация», «фейковая информация», «провокационная информация», «заведомо ложная информация», «компьютерные преступления» (связанные с компьютерной информацией), «информационные войны» и т.д. Они используются не только в научной литературе, но и в нормативно-правовых и подзаконных актах, политико-правовых документах, актах мягкого права, а также в текстах, направленных на популяризацию науки[2].

Например, «компьютерная информация» используется в ст. 272–274[2] УК РФ, «заведомо ложная информация» – в ст. 207[1], 207[2] УК РФ,

---

[1] Об информации, информатизации и защите информации: Федеральный Закон от 20 февраля 1995 г. № 24-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5887/ (дата обращения: 20.10.2023 г.). Утратил силу.

[2] Лихачев Н.А. Уголовно-правовые меры противодействия преступлениям, связанным с посягательствами на персональные данные граждан // Уголовно-правовые меры противодействия служебным, экономическим и иным преступлениям: современное состояние и пути оптимизации: Международная научно-практическая конференция (юридический факультет Ярославского государственного университета им. П.Г. Демидова, г. Ярославль, 30.09-1.10.2022 г.). С. 84.

«персональные данные». Последние регулируются профильным Федеральным законом[1], который определяет их как абсолютно любую информацию, относящуюся косвенно или прямо к конкретному субъекту персональных данных (физическому лицу)[2]. Законодатель использует широкий подход и в данном случае, так как исчерпывающие критерии не определены должным образом. В русском языке слово «косвенный» принято определять как «не непосредственный, побочный, не прямой»[3].

Отечественное и зарубежное законодательство давно развивается в направлении минимизации элементов неточности, казуистичности и неопределенности диспозиций правовых норм. В некоторых нормах, действительно, используется слово «косвенный», в частности в ч. 3 ст. 25 УК РФ. Уголовно-процессуальное право предусматривает возможность собирания и использования косвенных доказательств. Однако в этих случаях законодатель четко детерминирует оба термина, наделяя их конкретными признаками и критериями (ч. 3 ст. 25 УК РФ, гл.10 УПК РФ[4]).

Неопределенность понятия «персональные данные» создает трудности при квалификации преступлений на практике, в частности, по ст. 137 УК РФ. Ключевым и практически единственным критерием персональных данных, согласно Закону, является то, что это – информация. Следовательно, на данные, которые предположительно относятся к категории персональных, в теории должны распространяться требования ч. 1 ст. 2 ФЗ № 149. Получается, что признак «косвенности» позволяет при должном желании и соответствующей аргументации отнести к персональным данным абсолютно любую информацию.

---

[1] О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 06 февраля 2023 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_61801/ (дата обращения: 14.06.2023 г.).

[2] Там же.

[3] Кузнецов С.А. Современный толковый словарь русского языка. М.: Издательский дом Ридерз Дайджест, 2004. С. 293.

[4] Уголовно-процессуальный кодекс Российской Федерации 2001 г. (ред. от 23 марта 2024 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/ document/cons_doc_LAW_34481/. (дата обращения: 25.03.2024 г.).

Действующая редакция ч. 1 ст. 3 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ активно критикуется в научном сообществе по причине отсутствия формально-определённых критериев понятия, а также необходимости его сужения в целях повышения эффективности административно и уголовно-правовой защиты персональных данных граждан РФ[1].

Нормативно-правовое регулирование режима персональных данных в российском законодательстве должно предусматривать исчерпывающий перечень относящейся к ним информации, который бы дополнялся по мере необходимости. В него стоило бы включить:

– фамилию, имя, отчество, место, год рождения;

– данные документа, удостоверяющего личность;

– адрес регистрации и фактического проживания лица, номера мобильных и рабочих телефонов, сведения о работе, собственности (в том числе, зарегистрированном движимом и недвижимом имуществе);

– данные о приобретении авиа/жд. Билетов, сведения о перемещении субъекта персональных данных, в том числе о пересечении Государственной границы РФ;

– данные пенсионного фонда;

– данные трудового договора субъекта персональных данных;

– сведения, характеризующие физиологическое состояние лица (вес, рост, состояние здоровья, показатели выносливости и т.д.);

– материалы (фотографии, записи и иные сведения), размещенные пользователем на персональной странице в социальных сетях и иных информационных платформах;

– данные cookie, собирание истории геолокации и передвижения,

[1] См., напр.: Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 186-196; Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в Европейском контексте // Труды Института государства и права РАН. 2018. № 5. С. 117-150.

использования персональных электронных устройств.

Следовательно, неправомерное собирание и получение доступа к таким данным, их последующий незаконный оборот должны влечь уголовную ответственность. В настоящий момент в ИТС «Интернет» можно встретить большое количество информационных ресурсов, которые на возмездной или безвозмездной форме осуществляют сбор или оборот личных данных пользователей. За определенную сумму любой желающий может получить компиляцию сведений о физическом лице, находящихся в свободном доступе. Подобные поисковики позволяют установить место жительства человека, его круг общения, данные документов, удостоверяющих личность, недвижимое и движимое имущество, кредитную историю и т.д. Таким образом, частная жизнь гражданина ставится под угрозу, подобная противоправная деятельность представляет особую опасность для сотрудников правоохранительных органов и специальных служб и их семей, нарушая их права.

Проблематика определения персональных данных, их тесная взаимосвязь с рядом составов преступления плавно перетекает в вопросы нормативно-правовой охраны личной и семейной тайны. Действующее законодательство, несмотря на конституционно-правовую гарантию обеспечения такой тайны, не содержит легального определения указанных правовых категорий. Этот пробел в праве оказывает негативное влияние на уголовно-правовую охрану частной жизни физических лиц, вызывает сложности и неопределенности в квалификации преступлений. Акты судебного толкования тоже не содержат однозначного ответа, какую именно информацию следует относить к персональным данным.

Так, постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 содержит только пояснения относительно собирания и распространения сведений о частной жизни, не конкретизируя, что следует понимать под

частной жизнью лица применительно к соответствующим статьям УК РФ[1].

Единственную попытку дать на официальном уровне содержательное пояснение личной и семейной тайне предпринял Конституционный Суд РФ. В его определении от 28 июня 2012 г. № 1253-О указывается, что само лицо вправе определять, что именно относится к его личной, семейной тайне, вследствие этого сбор, хранение, распространение и использование информации о лице без его непосредственного согласия не допускается на основании положений Конституции Российской Федерации[2]. Отсутствие четких критериев личной и семейной тайны вызывает неопределенность в установлении соотношения этих понятий с персональными данными: пересекается ли предмет их правового регулирования, насколько эти данные тождественны, охватывает ли уголовно-правовая охрана личной тайны охрану персональных данных и наоборот. Возникает вопрос: противоправные действия с какими именно персональными данными имеют высокий уровень общественной опасности, соразмерно ли количественное посягательство на личную и семейную тайну степени тяжести преступного деяния.

Отметим, что терминологические проблемы определения информации и смежных понятий не являются уникальными для российского правового и научного пространства. Так, об общемировом философском кризисе в вопросе толкования определения информации свидетельствует мнение, представленное в трудах президента Международного общества изучения информации (IS4IS) Марцина Дж. Шредера, согласно которому существует большое количество разнообразных способов исследования информации,

---

[1] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.[1], 139, 144.[1], 145, 145.[1] Уголовного кодекса Российской Федерации): постановление Пленума Верховного Суда РФ от 25 декабря 2018 № 46 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_314616/. (дата обращения: 14.01.2024 г.).

[2] Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации: Определение Конституционного Суда РФ от 28 июня 2012 № 1253-О // СПС «Гарант». URL: https://www.garant.ru/products/ipo/prime/doc/70105530/ (дата обращения: 20.10. 2023 г.).

что соответственно приводит к расхождению в ее толковании. Ученый отмечает использование относительно пространных и нечетких понятий информации[1].

Действительно, в юридической науке можно выявить внушительное количество различных подходов к формулировке понятия «информация». Так, например, В.Г. Семенова и Е.А. Петриченко раскрывают ее как форму передачи человеческого опыта и знаний[2]. Тем самым авторы охватывают максимальный перечень объектов материального и нематериального мира, относимых к предмету определения.

А.Г. Волеводз отмечает, что юридическим критерием информации является документарная информация, содержащаяся на материальном электронном носителе, обладающая реквизитами, позволяющими ее идентифицировать[3].

Определяя сущность и правовое содержание информации, необходимо обратиться к действующим механизмам ее правового регулирования. Так, Конституцией Российской Федерации (далее – Конституция РФ) гарантируется право на свободный поиск, обработку, хранение, получение и распространение информации любым законным способом. Основной закон государства гарантирует также охрану тайны частной жизни, личной и семейной тайны (ст. 23), тайны переписки, переговоров, почтовых, телеграфных и иных сообщений (ст. 23) и государственной тайны (ст. 29)[4].

Обобщая конституционно-правовое содержание «информации»,

---

[1] Schroetter M Invariaiice as a Tool for Ontology of Information // Information. 2016. № 7-1 (11). P. 2-20.

[2] Семенова В.Г., Петриченко Е.А. Информация: история понятия, его настоящее и будущее // Известия вузов. Северо-Кавказский регион. Серия: Общественные науки. 2022. №1 (213). С. 23.

[3] Волеводз А.Г. Противодействие компьютерным преступлениям. М.: Юрлитинформ, 2002. С. 45.

[4] Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020) // СПС «КонсультантПлюс». URL: http://www.co№sulta№t.ru/docume№t/co№s_doc_LAW_28399/. (дата обращения: 14.01.2023 г.).

отметим, что любая форма тайны как юридической категории (личная, семейная, коммерческая, государственная, медицинская и т.д.) по своей сути представляет совокупность различных данных. Таким образом, информацию как официальный термин и правовое явление следует подразделять на:

– информацию, относящуюся к различным формам тайны;

– информацию, относящуюся к персональным данным;

– юридически значимую или правовую информацию;

– информацию, на которую распространяются требования авторского или патентного права.

Дополнительно информацию как правовую категорию можно классифицировать по юридическому критерию допуска к распространению:

– свободно распространяемая информация;

– информация, распространение которой допускается и происходит по соглашению сторон в ходе реализации правоотношений;

– информация, распространение которой производится или должно производиться на основании норм федерального или регионального законодательства;

– ограниченная или запрещенная к распространению информация (сведения, составляющие определенные формы тайны, социально опасная или противоправная).

Говоря о признаках информации как предмета информационных отношений, выступающих объектом уголовно-правовой охраны, необходимо отметить в первую очередь следующие:

– нормативность, то есть к влекущим уголовную ответственность относятся деяния, совершаемые только в отношении тех сведений, статус и значимость которых регулируется нормами действующего законодательства;

– достоверность, то есть объективность и правдивость изложенных

сведений в искомой информации;

– конфиденциальность: это должна быть определенная совокупность сведений вне зависимости от формы их представления и содержания, сокрытая от доступа неопределенного круга лиц в целях обеспечения и защиты прав конфидента, нарушение чего влечет наступление юридической ответственности того или иного вида;

– направленность – информация в процессе ее передачи или распространения способна оказывать эмоционально-психологическое воздействие на человека, социальную группу или общность людей, побуждать к совершению определенных действий или же наоборот – воздерживаться от совершения активно-волевых поступков;

– тайность, предполагающая законодательное императивное ограничение доступа неограниченного круга лиц к информации, имеющей особую государственную, медицинскую, коммерческую и иную ценность. Нарушение порядка хранения, обращения, передачи информации, имеющей тот или иной гриф тайны, влечет наступление уголовной ответственности.

Таким образом, необходимо различать технические, философские и юридические подходы к определению этой дефиниции. Информация в большинстве случаев выступает объектом/предметом отношений, регулируемых различными отраслями права. Для эффективной уголовно-правовой охраны общественных отношений, связанных с созданием, распространением, защитой информации, первостепенной задачей является выработка исчерпывающих признаков, характеризующих информацию и смежные понятия. Вследствие этого закономерна необходимость анализа правовой категории, имеющей непосредственное отношение к исследуемой теме, – информационной безопасности.

Правовое обеспечение информационной безопасности является структурным элементом общей теории национальной безопасности Российской Федерации, формирование которой началось еще в начале 90-х гг. XX в.

До этого в законодательной и научной практике был широко употребим иной термин – государственная безопасность, возникший в XIX в. О важности правового (в том числе уголовно-правового) обеспечения безопасности писал М.М. Сперанский, употребляя оборот «общей безопасности лиц», определяя категорию «внутренней государственной безопасности». Он характеризовал ее полицейскими мерами пресечения и предупреждения в целях обеспечения безопасности человека от различных посягательств. Кроме того, выделялась «общественная безопасность» как «сохранение вещей в том порядке, в каком они поставлены законом». Таким образом, угрозой безопасности является либо противоправное посягательство, либо злоупотреблением правом/законом[1].

В советском законодательстве приоритетным был подход к определению и обеспечению безопасности также с позиции защиты государственности. Термин «государственная безопасность» был включен в текст Конституции СССР 1936 г. (п. «и» ст. 14 гл. 2)[2]. Таким образом, главным объектом политики правового обеспечения безопасности была протекция государства и общества, существовавшего политического и конституционного строя уголовно-правовыми средствами.

Впервые в правой системе Российской Федерации официальное закрепление понятия «безопасность» как базовой категории в системе защиты прав и свобод человека и гражданина было осуществлено в 1992 г. в Законе РФ «О безопасности». После продолжительной дискуссии была принята формулировка следующего содержания – это «состояние защищенности

[1] Сперанский М.М. План государственного преобразования графа М.М. Сперанского (Введение к уложению государственных законов 1809 г.) с приложением «Записки об устройстве судебных и правительственных учреждений в России» (1803 г.), статей «О государственных установлениях», «О крепостных людях» и Пермского письма к императору Александру // СПС «Гарант». URL: https://constitution.garant.ru/history/act1600-1918/3848894/ (дата обращения: 20.10. 2023 г.).

[2] Конституция (Основной закон) Союза Советских Социалистических Республик (утверждена постановлением Чрезвычайного VIII Съезда Советов Союза Советских Социалистических Республик от 5 декабря 1936 г.) (утратила силу) // СПС «Гарант». URL: https://constitution.garant.ru/history/ussr-rsfsr/1936/. (дата обращения: 14.01.2023 г.).

жизненно важных интересов личности, общества и государства от внутренних и внешних угроз». При этом «жизненно важные интересы» трактовались очень условно и расплывчато как некие потребности, направленные на существование и последующее развитие личности и общества. В то же время важным моментом в нормативном акте стало формирование комплексной архитектуры безопасности[1]:

– для человека – обеспечение и защита его непосредственных прав и свобод;

– для общества – создание, обеспечение и поддержание материальных и духовных ценностей;

– для государства – защита и поддержание конституционного строя, суверенитета и территориальной целостности от внешних и внутренних посягательств.

В 2010 г. был принят новый Федеральный закон № 390-ФЗ «О безопасности», модернизировавший и дополнивший систему обеспечения таковой. От предыдущего акта он отличается всеобъемлющим и концептуальным подходом. В Законе отсутствует определение безопасности, в ст. 1 определяется лишь предмет регулирования – «деятельность по обеспечению безопасности/национальной безопасности». Дополнительно введена статья, посвященная международному сотрудничеству в сфере обеспечения безопасности. Статьи 2 и 4 вводят интересную новеллу – государственную политику в области обеспечения безопасности. Законодатель отмечает, что деятельность по обеспечению безопасности носит не только юридический (уголовно-правовой, уголовно-процессуальный), но и политический характер[2]. Государственная политика

[1] О безопасности: Закон РФ от 5 марта 1992 г. № 2446-I (с изм. и доп.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru /document/cons_doc_LAW_376/ (дата обращения: 20.10. 2023 г.). Утратил силу.

[2] О безопасности: Федеральный закон от 28 декабря 2010 г. № 390-ФЗ (ред. от 10 июля 2023 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_108546/ (дата обращения: 14.10.2023 г.).

в области обеспечения безопасности, ее основные направления определяются Президентом Российской Федерации. На основании этих законов принимались подзаконные акты, регулирующие практику обеспечения безопасности в различных сферах:

– о стратегии национальной безопасности (указы Президента РФ от 2009 г. № 537[1], от 2016 г. № 683[2], от 2021 г. № 400[3]);

– доктрины отраслевых направлений обеспечения безопасности (информационная, военная, экологическая и т.д.).

Данные акты носят концептуальный политико-правовой характер, определяют роль и место Российской Федерации в мире, основные вызовы и угрозы национальной безопасности России, меры и направления обеспечения таковой. Стратегии и доктрины, несмотря на обязательную юридическую силу и статус главного подзаконного акта в государстве, являются более политическими, нежели правовыми документами. Они определяют вектор развития отрасли на конкретный, отраженный в них период и должны оказывать воздействие «мягкой силы» на внутреннюю и внешнюю целевую аудиторию (политические и экономические элиты, бюрократический аппарат, правоохранительную систему и т.д.).

Одним из таких актов является Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»[4]. Он содержит следующее определение

[1] О Стратегии национальной безопасности Российской Федерации до 2020 года: Указ Президента РФ от 12 мая 2009 г. № 537 (ред. от 01 июля 2014 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_87685/ (дата обращения: 20.10.2023 г.). Утратил силу.

[2] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31 декабря 2015 г. № 683 // СПС «КонсультантПлюс». URL: http://www.consultant.ru /document/cons_doc_LAW_191669/ (дата обращения: 20.10. 2023 г.). Утратил силу.

[3] 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.).

[4] Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208191/ (дата обращения: 14.01.2023 г.).

информационной безопасности – состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства.

В последние годы вопросы обеспечения информационной безопасности приобрели ключевое значение в силу роста уязвимости в геометрической прогрессии безопасности, сохранности и конфиденциальности данных. В результате научной полемики возникло большое количество различных подходов и определений информационной безопасности. Когда трансформация современных общественных отношений в результате цифровизации, роста объема ежедневно обмениваемой и создаваемой информации стала очевидна, возникла острая необходимость в уголовно-правовой охране прав личности, общества и государства, связанных с хранением, передачей, обработкой, распространением информации. Однако в настоящий момент на уровне федерального законодательства (в частности, в ФЗ № 149) анализируемый термин отсутствует, хотя официально-правовой статус он приобрел еще в 2000 г. в Доктрине от 9 сентября 2000 г. № Пр-1895[1].

Исходя из анализа официального определения, можно сделать вывод, что информационная безопасность является частным понятием по отношению к национальной безопасности. В то же время представляется ошибочным отождествление понятий национальная безопасность и безопасность в целом, так как первое определение обладает национальным специфическим аспектом (защита языка, культуры, сохранение традиций и обычаев отдельных народов,

[1] Доктрина информационной безопасности Российской Федерации: утв. Президентом РФ 09 сентября 2000 г. № Пр-1895 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_28679/ (дата обращения: 14.01.2023 г.).

защита народов и наций от геноцида, уголовно-правовая защита от преступлений террористической и экстремисткой направленности, а также от иных преступлений по национальному признаку), а понятие безопасности носит более широкий характер, охватывающий интересы и права граждан РФ. Что касается информационной безопасности как части государственной политики по обеспечению безопасности, то она нацелена на реализацию положений ст. 23–29 Конституции РФ, а также на уголовно-правовую защиту от ряда преступлений, предусмотренных нормами Особенной части УК РФ[1].

Одним из первых ученых, предметно исследовавших проблемы обеспечения информационной безопасности и формулировавших собственное понятие информационной безопасности, был В.Н. Лопатин. Именно его определение легло в основу Доктрины информационной безопасности Российской Федерации 2000 г. Анализируя сущность информационной безопасности, В.Н. Лопатин отмечает, что ее обеспечение и защита займут центральное место в системе национальной безопасности на ближайшие десятилетия[2].

Большинство ученых рассматривают информационную безопасность как целостную систему, состоящую из совокупности различных элементов. Так, А.А. Малюк понимает ее как систему, которая направлена на противодействие внешним и внутренним угрозам и в то же время сама не является угрозой (технический подход к информационной безопасности)[3].

Однако рассмотрение информационной безопасности как явления исключительно технического, то есть как процесса технического

---

[1] Лихачев Н.А. Современная уголовная политика Российской Федерации в сфере обеспечения информационной безопасности // Прогресс и преемственность в российском уголовном праве (к 95-летию УК РСФСР 1926 г. и 25-летию УК РФ 1996 г.): Всероссийская научно-практическая конференция с международным участием (Кубанский государственный университет, г. Краснодар, 28-29.05.2021 г.). Краснодар, 2021. С. 639.

[2] Лопатин В.Н. Информационная безопасность России: автореф. дис. … д-ра юрид. наук. СПб., 2000. С. 6–7.

[3] Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учебное пособие для вузов. М.: Горячая линия. Телеком, 2004. С. 42.

и технологического обеспечения конфиденциальности данных на электронных (компьютерных) носителях, представляется ошибочным. Информационная безопасность представляет собой многоплановое социальное явление, динамичную, а не статичную систему. Она должна быть направлена не только на обеспечение сохранности оцифрованных данных, но и на процессы и специфические особенности сбора и распространения информации.

Схожей позиции придерживается Т.В. Закупень, отмечая, что информационная безопасность – это социальное, а не техническое явление и ее нельзя охарактеризовать как процесс применения специальных технических средств, направленных на защиту информации от внешнего и внутреннего воздействия[1].

Помимо определения информационной безопасности в уголовно-правовой науке часто применяется понятие кибербезопасности, в некоторых случаях они рассматриваются как синонимичные. Дефиниция «кибербезопасность» пришла в отечественный научный дискурс из европейской и американской юридической науки. Она является логическим продолжением развития науки кибернетики, посвященной общим законам получения, хранения, передачи и преобразования информации в сложных управляющих системах[2].

В российском уголовном законодательстве не используются понятия кибербезопасности, киберпространства, киберпресутпности, хотя в некоторых подзаконных актах политико-правового характера подобные определения встречаются. Например, в п. 17 Концепции внешней политики Российской Федерации 2016 г. киберпреступность раскрывается как трансграничный

[1] Закупень Т.В. Понятие и сущность информационной безопасности и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. № 4. С. 28–34.

[2] Глушков В. М. Амосов Н.М. Артеменко И.А. Энциклопедия кибернетики. Киев: Главная редакция украинской советской энциклопедии, 1974. С. 440.

вызов и угроза безопасности Российской Федерации[1]. При этом ни в положениях главы 28 УК РФ, ни в постановлениях Пленума Верховного Суда РФ, ни в обзорах судебной практики данные определения не встречаются.

Некоторые ученые объясняют неоднородность использования уголовно-правовой терминологии в сфере уголовной ответственности за нарушение информационной безопасности релевантностью при переводе с английского на русский язык[2].

Представляется, что уголовно-правовое обеспечение информационной безопасности сегодня 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-телекоммуникационных систем, сайтов, информационных ресурсов и объектов критической информационной инфраструктуры;

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

Важно понимать, что информационная безопасность – это не статичное явление, так как зачастую представляет опасность не только нарушение целостности и конфиденциальности любых данных – от государственной тайны до личной и семейной тайны отдельно взятого гражданина, но и последующее распространение информации. В частности, публикация каких-либо данных (о нем или о его семье или близких) может быть

[1] Об утверждении Концепции внешней политики Российской Федерации: Указ Президента РФ от 30 ноября 2016 г. № 640 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_207990/. (дата обращения: 14.01.2023 г.).

[2] Касенова М.Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. ... д-ра юрид. наук. М., 2016. С. 27.

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

В ИТС «Интернет» созданы и распространяются приложения и информационные платформы, которые направлены на собирание различных данных по запросу, что формирует, по сути, своеобразное досье из личных данных гражданина, его места жительства, телефонов, паспортных данных, телефонной книги, историй поиска в интернете, фото и видеофайлов с ним и т.д.

Нельзя обойти вниманием и информационный экстремизм – относительно новое в юридической и уголовно-правовой науке понятие, характеризующее действия, направленные на умышленную дискредитацию физического лица путем проведения против него информационной кампании (публикации заведомо ложных, недостоверных или частично ложных сведений, манипуляции информацией и сведениями и т.д.).

Думается, что перечисленные явления также подпадают под определение, а следовательно, под предмет правового регулирования в рамках информационной безопасности. Исходя из этого, понятие *информационной безопасности* следует определить как состояние динамически развивающейся системы защиты информации и информационных прав граждан и предупреждения от преступных посягательств на них.

По субъекту информационную безопасность необходимо дифференцировать на личную, общественную, государственную и международную. При этом каждый из элементов имеет тесную взаимосвязь с другими. Во многом это продиктовано тем, что государство обеспечивает информационную безопасность личности и общества посредством процессуальной деятельности правоохранительных органов и иных государственных механизмов. Физические лица, совершая отдельные преступления, предусмотренные УК РФ, фактически наносят существенный

вред информационной безопасности личности, общества и государства, что выражается в конкретных общественно опасных последствиях.

Таким образом, анализируя различные мнения и подходы к пониманию информации и информационной безопасности, следует констатировать отсутствие их единства. Информацию воспринимают и как объект информационных отношений, и как процесс. В то же время практически полностью отсутствует юридическое понимание информации как правовой категории. Информации как одному из наиболее общеупотребимых терминов (встречается более чем в 18 кодексах российского права) требуются конкретизация и пояснение. Для эффективного уголовно-правового обеспечения информационной безопасности в первую очередь необходимо привести понятийно-категориальный аппарат действующего федерального законодательства в соответствие с актуальными запросами и требованиями времени. Следует четко определить понятие информации, персональных данных, личной и семейной тайны, частной жизни лица, выделив их критерии и признаки, чтобы отграничить любую информацию от той, которая подлежит уголовно-правовой охране.

Таким образом, исследовав различные существующие подходы к определению понятия и сущности информации и информационной безопасности в уголовно-правовой сфере, можно предложить следующее доктринальное определение информации – это являющиеся объектом уголовно-правовой охраны, содержащие персональные данные или относящиеся к любой разновидности тайны, порядок допуска к которым, в том числе ознакомление с ними, их распространение, копирование, изменение, уничтожение, а также порядок и форма хранения, подлежит императивному правовому регулированию, нарушение которого влечет уголовную ответственность.

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

– оценку эффективности, соразмерности, целесообразности

действующих норм уголовного законодательства, в случае необходимости – осуществление криминализации или декриминализации тех или иных деяний в информационной сфере;

– организацию взаимодействия уголовно-правовых, уголовно-процессуальных, криминалистических мер, направленных на более эффективное применение норм уголовного права;

– эффективное уголовно-правовое противодействие преступлениям против информационной безопасности, а также их предупреждение и профилактика путем повышения правовой грамотности в обществе (подробнее об этом в следующем параграфе диссертации);

– прогнозирование и оценка тенденций развития преступности в сфере информационной безопасности с учетом научно-технического прогресса, достижений других научных областей в области хранения, обеспечения, передачи информации.

1.2 Уголовно-правовое обеспечение информационной безопасности в Российской Федерации

Научный прогресс, рост доступности электронных устройств для коммуникации, повсеместное распространение ИТС «Интернет», всеобъемлющая цифровизация и создание национальных реестров, содержащих данные граждан, привело к качественному изменению отношений в информационной сфере. В результате сформировалась новая среда для взаимодействия между субъектами создания, распространения, передачи и воздействия информации. Это значительно ускорило процессы ее распространения, а следовательно, недостоверная, заведомо ложная, социально опасная информация стала более доступной, а все противоправные действия, связанные с ней, приобрели широкую распространенность и высокий уровень общественной опасности.

Определив информационную безопасность как динамически

развивающуюся систему защиты информации и информационных прав граждан от преступных посягательств и их предупреждение, необходимо установить место информационной безопасности в системе уголовно-правовых отношений.

Информационная безопасность, равно как и ее обеспечение, представляет собой в первую очередь совокупность общественных отношений, которые объединяют общие признаки. В уголовно-правовой науке информационная безопасность также определяется как система общественных отношений. Связано это в первую очередь с тем, что под объектом преступного посягательства в подавляющем большинстве случаев понимаются общественные отношения, которые охраняются уголовным законом.

Существует большое количество подходов к определению преступлений в сфере информационной безопасности, сформировавшиеся в устойчивые классификации. Так, одна из них предполагает узкий подход к трактовке преступлений в сфере информационной безопасности и выделяет две основные группы[1]:

– «традиционные» преступления – при совершении указанных деяний информационные технологии выступают лишь инструментом совершения преступного посягательства (кража, мошенничество и т.д.);

– Компьютерные преступления, существенной особенностью которых является возможность совершения деяния исключительно посредством применения различных информационных технологий (DdoS-атака, взлом баз данных, страниц в социальных сетях, электронных почт, осуществление иных действий, направленных на получение неправомерного доступа к компьютерной информации);

– преступления, связанные с информацией, представленной

[1] Жижина М.В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. М.: Проспект, 2022. С. 9.

вне цифровой (компьютерной) формы.

Понятие компьютерных преступлений толкуется весьма широко и является предметом научной дискуссии.

Отметим, что данная трактовка не является единственной и универсальной, ряд ученых использует другое понятие – киберпреступность или киберпреступления. Так, В.Н. Цимбал и С.Г. Клюев определяют киберпреступление как противоправное деяние в сфере информационных технологий, совершаемое при помощи указанных технологий в глобальных и локальных вычислительных сетях[1]. И.В. Романов раскрывает понятие киберпреступления через термин киберпространства, определяя его как общественно опасное деяние, но уже совершаемое в киберпространстве, посягающее на общественную безопасность, права человека и иные охраняемые законом отношения, где предметом преступного посягательства и средством совершения преступления выступает компьютерная информация[2].

Всего же можно выделить более 10 различных доктринальных подходов к определению киберпреступления, носящих как широкий характер, предполагающий большое количество различных преступных деяний в данной сфере, так и узкий, охватывающий ограниченное, усеченное количество преступлений.

Отметим, что официального правового определения понятий киберпреступности и киберпреступления в отечественной правовой системе нет. Как отмечалось ранее, происхождение этих терминов восходит к науке кибернетике, а также международному и зарубежному праву, в частности, к Европейской конвенции о киберпреступности[3], которую Российская

[1] Цимбал В.Н., Клюев С.Г. Понятие киберпреступления и его содержательная часть // Вестник Московского университета МВД России. 2021. № 1. С. 130.

[2] Романов И.В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 105-109.

[3] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС КонсультантПлюс. URL:

Федерация не стала подписывать в силу различных причин.

Среди прочих можно выделить подходы С.И. Буз[1], Л.И. Бутовой[2], Д.Н. Карпова[3], Э.Л. Кочкина[4], В.А. Номоконова[5], Е.С. Шевченко[6] и др.

На законодательном уровне в гл. 28 УК РФ используется понятие «Преступления в сфере компьютерной информации». Одним из первых авторов такого понятия в науке уголовного права явилась Т.Г. Смирнова, которая определила соответствующее преступление как запрещенное уголовным законом общественно опасное деяние, причиняющее вред либо создающее угрозу причинения вреда жизни, здоровью личности, правам и законным интересам человека и гражданина, государственной и общественной безопасности[7].

Актуальным остается вопрос соотношения двух понятий – «преступления в сфере компьютерной информации» и «компьютерные преступления», так как формулировка существенным образом влияет на квалификацию и содержание составов преступлений, предусмотренных гл. 28 УК РФ. Связано это с необходимостью точного определения видового объекта и в отдельных случаях предмета преступного посягательства, предусмотренного ст. 272–274[2] УК РФ.

Представляется, что преступления в области информационной

---

https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526&ysclid=lucmtjcx1541169722#Ge2dP8UuhrfJ5B011 (дата обращения: 14.01.2023 г.).

[1] Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ – Правоведъ. 2019. № 4 (91). С. 78.

[2] Бутова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник. 2016. № 3 (15). С. 28-31.

[3] Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46-50.

[4] Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162-169.

[5] Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45-55.

[6] Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук. М., 2016. С. 96.

[7] Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. М., 1998. С. 6.

безопасности следует толковать шире, включая все уголовно-правовые деликты, нарушающие информационные права человека и гражданина, а не только те, что указаны в гл. 28 УК РФ.

Что же касается определения преступлений в сфере компьютерной информации, то ряд исследователей поддерживает позицию законодателя, который включает в предмет преступного посягательства не только компьютерную информацию, но и сам компьютер, компьютерную сеть, критическую инфраструктуру (ст. 274[1] УК РФ). В частности, такой позиции придерживались Г.Н. Борзенков и В.С. Комиссаров[1].

Существует и иная точка зрения, согласно которой преступное деяние, представляющее собой направленное воздействие на компьютерное устройство с целью его повреждения, уничтожения, выведения из строя, по родовому признаку объекта преступления следует относить к преступлениям против собственности (гл. 21 УК РФ).

В случае, если происходит применение вредоносной компьютерной программы, результатом которой является копирование, изменение, уничтожение компьютерной информации, сопровождающейся уничтожением, повреждением выведением из строя компьютерного устройства, данные деяния следует квалифицировать по совокупности или же определять приоритетную направленность умысла, что было первичной целью – информация или уничтожение.

Подобной точки зрения придерживался Ю.И. Ляпунов[2].

Н.Н. Коротких полагает, что преступные посягательства на компьютеры и компьютерные сети не могут быть отнесены к преступлениям в сфере компьютерной информации, взамен предлагается создание отдельной категории преступлений – «компьютерных преступлений». Автор отмечает,

---

[1] Курс уголовного права: в 5 т. Т. 4 / под ред. Г.Н. Борзенкова, В.С. Комиссарова. М.: Зерцало, 2002. С. 317.

[2] Ляпунов Ю.И. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 8-15.

что под компьютерными понимаются преступления, подразумевающие использование компьютера в любом виде, без ограничения рамками компьютерной информации[1].

М.В. Жижина, анализируя соотношение понятий компьютерных преступлений и преступлений в сфере компьютерной информации, оценивает их как целое и часть. Объект последних являются видовым в соотношении с родовым объектом компьютерных преступлений. Понятие киберпреступления автор считает синонимичным компьютерным преступлениям[2].

А.Н. Попов, оценивая понятие «компьютерные преступления», рассматривает его в трех аспектах[3]:

– как синонимичное понятию «преступлениям в сфере компьютерной информации»;

– как определение той категории преступлений, которые совершаются в сфере информационной-телекоммуникационных технологий (информационные преступления);

– как определение преступлений, совершаемых с помощью компьютерных технологий (компьютерных систем/сетей) против других компьютерных систем/сетей.

Отметим, что данная классификация, безусловно, представляет научный и практический интерес, однако представляется, что применение понятия «информационные преступления» в данном случае ошибочно. Информационные преступления не охватываются исключительно компьютерными или цифровыми преступлениями, так как способы хранения,

---

[1] Коротких Н.Н., Останин М.Д. К вопросу о соотношении понятий «преступление в сфере компьютерной информации» и «компьютерное преступление» // Азиатско-Тихоокеанский регион: экономика, политика, право. 2018. № 3. С. 73.

[2] Жижина М.В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. М.: Проспект, 2022. С. 10.

[3] Попов А.Н. Преступления в сфере компьютерной информации: учеб. пос. СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. С. 6.

обмена и передачи информации не ограничивается электронными носителями. Под информационными преступлениями следует понимать те деяния, которые предполагают совершение посягательства на информационные права граждан.

Имеет место и научная дискуссия относительно выделения в самостоятельную категорию преступлений, связанных с посягательствами в виртуальном пространстве, если точнее, в ИТС «Интернет». Так, Р.И. Дремлюга придерживается позиции, согласно которой преступления в сфере компьютерной информации не всегда можно охарактеризовать как интернет-преступления, но каждое интернет-преступление – компьютерное[1]. Данный тезис обосновывается следующим доводом: способом и средством совершения преступления в сфере компьютерной информации как свойством объективной стороны состава преступления не всегда может быть ИТС «Интернет». Однако, если в случае совершения преступного посягательства используется ИТС «Интернет», это можно учитывать как особое отягчающее обстоятельство или основание для дополнительной квалификации.

И.Р. Бегишев выделяет преступления в сфере обращения цифровой информации как общественно опасные деяния, направленные на нарушение конфиденциальности, целостности, доступности и достоверности охраняемой законом информации[2]. При этом делается акцент не на компьютерную составляющую состава преступления, а на информационную – безопасность цифровой информации как видовой объект посягательств, предусмотренных УК РФ.

Проблема отграничения понятий «компьютерные преступления», «преступлений в сфере информационной безопасности», «преступления против компьютерной информации», «It-преступления» как деяний,

[1] Дремлюга Р.И. Интернет-преступность: монография / под ред. В.Г. Дроздова. Владивосток: Изд-во Дальневост. ун-та, 2008. С. 51.

[2] Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: автореф. дис. ... канд. юрид. наук. К., 2017. С. 19.

направленных на нарушение информационной безопасности, корреспондирует с проблемами квалификации имеющихся составов преступлений, предусмотренных нормами УК РФ, и деяний, криминализация которых активно обсуждается в профессиональном сообществе. В частности, не определено место кибератак и террористических актов в киберпространстве в уголовном праве. IT-преступления постепенно интегрируются с преступлениями, совершаемыми с сфере высоких технологий, из-за развития технологий искусственного интеллекта, дипфейков и иных программ, направленных на изменение и подделку биометрических данных пользователей.

УК РФ в действующей редакции выделяет три группы компьютерных преступлений:

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

– преступления, связанные с использованием компьютерной техники или оборудования как способа совершения преступления общеуголовного характера (например, ч. 3 ст. 141, ст. 159^6 УК РФ и др.);

– преступления общеуголовного характера, которые совершаются 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 составы преступлений, представленные в рамках данной классификации, следует относить к преступлениям против информационной безопасности в силу содержания их объекта. Некоторые компьютерные преступления можно рассматривать как вид преступлений, посягающих на информационные отношения.

Учитывая сформировавшуюся систему национальной безопасности, неотъемлемой частью которой является выстраиваемая государством система информационной безопасности, преступления, которые определяются как «информационные», «компьютерные», «киберпреступления» и т.д.,

предлагается объединить в общую группу – «преступления против информационной безопасности» и определить как 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.

Помимо преступлений, сопряженных непосредственно с компьютерной информацией, уголовное законодательство обеспечивает охрану информационных прав граждан посредством установления ответственности за оборот социально опасной информации[1]:

– о способах совершения самоубийства и за призывы к ним;

– о несовершеннолетних, пострадавших в результате преступлений;

– направленной на вовлечение несовершеннолетнего в преступную деятельность;

– об обороте веществ, которые ограничены в свободном гражданском обороте;

– о способах и методах изготовления наркотических и психотропных веществ и средств;

[1] О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено (вместе с «Правилами создания, формирования и ведения единой автоматизированной информационной системы «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено», «Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети "Интернет", распространение которых в Российской Федерации запрещено»): постановление Правительства РФ от 26 октября 2012 г. № 1101 (ред. от 29 апреля 2023 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_207990/ (дата обращения: 22.11.2023 г.).

– о материалах порнографического характера, изготовленных с участием несовершеннолетних;

– нацистской, экстремистской и террористической символики, пропаганды и оправдания нацизма;

– призывы к массовым беспорядкам, нарушению территориальной целостности РФ, дискредитация органов государственной власти и Вооруженных Сил РФ;

– сведения, составляющие государственную тайну;

– заведомо ложные или недостоверные сведения, представляющие угрозу жизни, здоровью и безопасности граждан.

В некоторых случаях данная информация может выступать в качестве предмета преступного посягательства, а ее распространение, выраженное в публичном призыве, дискредитации или пропаганде, характеристикой объективной стороны состава преступления (содержание данного тезиса будет раскрыто во второй главе диссертации).

Предполагается, что информационную безопасность необходимо исследовать с позиции трех основных структурных компонентов:

– уголовно-правового (нормативная база, которая способна обеспечить охрану интересов и прав личности, общества и государства в информационном пространстве);

– информационно-технического (техническая и технологическая защита информации, компьютерных сетей, серверов, систем от неправомерного воздействия извне);

– информационно-психологического (защита личности и общества от негативного когнитивного и манипуляторного воздействия призывов, пропаганды, распространения недостоверной или заведомо ложной информации).

Современные отрасли научного познания все чаще исследуют человека сквозь призму нескольких составляющих, представляющих общее единство –

физическую, психофизиологическую и социальную. Информационное пространство как новая реальность в философском смысле и виртуальное пространство в техническом все чаще становятся местом совершения преступных посягательств, а информация или слово как средством совершения преступления, так и предметом посягательства.

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 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).

Уголовно-правовое реагирование на соответствующую деятельность в ИТС «Интернет» сегодня имеет, безусловно, ключевое развитие для науки, однако ни информация в частности, ни информационная безопасность в целом не ограничиваются виртуальной реальностью.

Правовое регулирование информационной сферы – это комплексная сложная и многоаспектная задача, представляющая собой синергию различных отраслей науки. При решении правовых коллизий, восполнении пробелов в уголовном законодательстве следует учитывать научные достижения и опыт информологии, журналистики, лингвистики, психологии, программирования, информатики, физики, политологии. Однако, прежде всего, приоритетной задачей на краткосрочную перспективу должно стать формирование устойчивого понятийно-категориального аппарата как для ряда статей УК РФ, так и для федерального законодательства, непосредственно направленного на обеспечение информационной безопасности государства.

1.3 Обеспечение информационной безопасности в международном уголовном праве

Преступления, совершаемые в сфере информационно-коммуникационных технологий, представляют собой транснациональную проблему. Они не имеют границ, для них не существует межгосударственных преград. Нынешний уровень развития компьютерных технологий и программирования позволяет совершить преступление, связанное с неправомерным доступом к компьютерной информации, хищением средств, нанесением иного вреда информационным сетям и объектам КИИ, находясь практически в любой точке земного шара. Именно поэтому эффективное

противодействие новой по своей сущности и философии форме преступности возможно только путем консолидации усилий всего мирового сообщества по типу противодействия, например, международному терроризму.

По различным оценкам, в 2022 г. ежесекундный поток Интернет-трафика в мире составлял 150700 гигабайт[1]. Тенденция к росту в перспективе не только сохранится, он будет увеличиваться пропорционально росту населения и ускорению цифровизации в развивающихся странах. Согласно статистике Social 2020, среднестатистический человек в среднем проводит в интернете 6 час. Ежедневно[2]. Рост цифрового потенциала является определяющим в будущем развитии государств, при определении их роли на международно-политической арене, степени их влияния, уровня жизни и благополучия населения.

В настоящее время международное, в том числе и международное уголовное, право переживают сложный период трансформации. Тем не менее, проблема международного обеспечения информационной безопасности возникла достаточно давно. Однако единого, универсального международного механизма противодействия подобного рода преступлениям все еще нет. Конечно, существуют отдельные институты и предпосылки для этого, межгосударственные позитивные политические отношения позволяют реализовывать институт экстрадиции и привлекать к уголовной ответственности лиц, совершивших преступления против информационной безопасности, находясь вне пределов Российской Федерации. Однако, к сожалению, эти случаи носят скорее частный, нежели системный характер.

Формирование международно-правового регулирования информационных отношений, создания, распространения, передачи, хранения

---

[1] Global Business Data Platform Statista. URL: https://www.statista.com/statistics/631151/worldwide-data-collected-by-smart-buildings/. P. 43-48 (дата обращения: 20.10.2023 г.).

[2] Вся статистика интернета на 2020 г. – цифры и тренды в мире и в России // Web Canape, 03.02.2020 г. URL: https:// www.web-canape.ru/business/internet-2020-globalnaya-statistika-i-trendy/ (дата обращения: 20.10. 2023 г.).

и защиты информации началось после окончания Второй мировой войны и построения действующей системы миропорядка, переживающей глобальный экзистенциальный кризис. На базе Организации Объединенных Наций (далее – ООН), а также Всеобщей декларации прав человека гарантировались права на свободу убеждений и вероисповеданий, свободу поиска, распространения и получения информации любыми законными способами и средствами. Информация постепенно стала трансграничным и вненациональным явлением. Закон также стал защищать частную и семейную жизнь человека от противоправных посягательств извне, что стало первыми шагами к построению архитектуры системы международной информационной безопасности.

Ученые в настоящее время по-разному оценивают степень развития международно-правого регулирования информационной безопасности. Так, В.П. Талимончик пишет о формировании на базе ООН концепции международной информационной безопасности, работе институциональных механизмов сотрудничества между государствами[1].

Н.П. Ромашкина указывает на наличие серьезных расхождений в позициях ведущих держав относительно международной системы информационной безопасности, приходя к выводу, что только путем компромиссов и взаимных уступок можно снизить угрозы безопасности в этой сфере[2].

В.П. Коняхин отмечает необходимость унификации видов компьютерных преступлений на национальном и международном уровнях в целях повышения эффективности борьбы с ними в общепланетарном масштабе[3].

---

[1] Талимончик В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Правоведение. 2008. № 2. С. 105-116.

[2] Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1 (29). С. 2.

[3] Коняхин В.П. Компьютерные преступления: компаративистский анализ // Научно-технологическое обеспечение агропромышленного комплекса России: проблемы

По мнению Т.Ю. Сидоровой, утрата ООН позиции ведущей международной платформы по разработке и принятию международных норм, обеспечивающих информационную безопасность, приведет к негативным последствиям – появлению ряда региональных конвенций и соглашений[1].

С данной позицией трудно не согласиться, поскольку появление нескольких региональных соглашений или конвенций неизбежно приведет к возникновению противоречий в трактовках, формированию различных составов преступлений и криминализации разных деяний. Это будет способствовать еще большему усложнению архитектуры современной международной информационной безопасности. К сожалению, события последних лет свидетельствуют о деградации ООН и Совета Безопасности ООН как ключевых международных платформ, занимающихся вопросами мира, международной стабильности и безопасности, а следовательно, и информационной безопасности.

Стремительное ускорение научно-технического прогресса вызывало реакцию со стороны государственно-правового регулирования отношений в сфере обращения и применения информационных технологий. Становилось очевидно, что бесконтрольный оборот информации представляет угрозу безопасности общества и государства. Так, 28 января 1981 г. была принята Конвенция Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»[2]. Уже в 1981 г. отмечалась тенденция трансграничного потока персональных данных,

---

и решения: сборник тезисов по материалам III Национальной конференции (Краснодар, 27–28 марта 2019 г.). Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. С. 184.

[1] Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН // Сибирский юридический вестник. 2020. № 3 (90). С. 107.

[2] О защите физических лиц при автоматизированной обработке персональных данных: Конвенция СЕ (заключена в г. Страсбурге 28 января 1981 г.) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15 июня 1999 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_121499/ (дата обращения: 20.04.2023 г.).

необходимость обеспечения неприкосновенности частной жизни и соотнесение это со свободой распространения информации, что прямо отражено в преамбуле.

Большую роль в продвижении идеи уголовно-правового регулирования обеспечения информационной безопасности на международном уровне играет Российская Федерация. Так, в 1998 г. в рамках ООН по предложению нашего государства была принята первая резолюция «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»[1]. Этот международно-правовой акт положил начало политико-правовой дискуссии относительно определения пределов допустимости использования современных информационно-коммуникационных технологий и распространения информации различного характера и содержания.

Впоследствии были принята Окинавская хартия глобального информационного общества от 22 июля 2000 г.[2] Значение этого документа заключается в том, что в нем информационные-коммуникационные технологии признаются ключевым фактором, определяющим развитие в XXI в. Пункт 5 анализируемого акта призывает суверенные государства к развитию информационных технологий, формированию партнерства между всеми участниками в этой сфере.

Современная международная архитектура противодействия преступлениям в сфере информационно-телекоммуникационных технологий во многом базируется на Конвенции Совета Европы о киберпреступности, подписанной в Будапеште в 2001 г. В результате принятия Протокола № 1 к данной Конвенции была официально определена правовая классификация

[1] Резолюция Генеральной Ассамблеи ООН A/RES/53/70 от 4 декабря 1998 г. // Официальный сайт ООН. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement (дата обращения: 20.04.2023 г.).

[2] Окинавская хартия глобального информационного общества от 21 июля 2000 г. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=8382#AuSltZTJodXDwttG (дата обращения: 20.04.2023 г.).

преступлений в сфере киберпреступности[1]:

1) преступления против конфиденциальности, целостности и доступности компьютерных данных и систем:

– противозаконный доступ;

– противозаконный перехват;

– воздействие на данные;

– воздействие на функционирование системы;

– противозаконное использование устройств;

2) правонарушения, связанные с использованием компьютерных средств:

– подлог с использованием компьютерных технологий;

– мошенничество с использованием компьютерных технологий;

3) правонарушения, связанные с содержанием данных:

– преступления, связанные с детской порнографией;

4) правонарушения, связанные с нарушением авторского права и смежных прав.

Конечно, с течением времени данная классификация несколько утратила свою актуальность в связи с появлением новых форм и объектов преступных посягательств, однако именно она отразила попытку части международного сообщества определить, что следует понимать под информационной преступностью и каким образом унифицировать национальное уголовное законодательство стран–подписантов Конвенции. Данная Конвенция неоднократно становился объектом исследования отечественных ученых, особенно в контексте интеграции международного опыта в отечественное уголовное законодательство[2].

---

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#s6sltZT8ojzV24w91 (дата обращения: 20.04.2023 г.).

[2] См., напр.: Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1; Ефремова М.А. Международно-правовые основы уголовно-правовой охраны информационной безопасности // Правосудие.

Российская Федерация так и не подписала данную Конвенцию, хотя количество стран-подписантов ежегодно растет (более 50 государств–участников). Позиция Российской Федерации заключается в принципиальном непринятии п. «b» ст. 32, исполнение которого влечет нарушение внутреннего информационного суверенитета государства, так как он предусматривает возможность «получать через компьютерную систему на своей территории доступ к хранящимся на территории другой Стороны компьютерным данным или получать их»[1].

Б.Н. Мирошников, характеризуя спорный пункт, отмечает, что ключевой позицией является политика невмешательства во внутренние дела суверенных государств, уважения прав и свобод человека и гражданина. Невозможно говорить о равном и взаимоуважительном сотрудничестве при условии, если одна сторона проводит специальные информационные операции на территории другой без ее согласия[2].

Иной точки зрения придерживается Е.А. Русскевич. Он выступает за подписание Российской Федерации конвенции, отмечая, что на сегодняшний день конвенция является самым проработанным и значимым международным документом, что отечественная уголовно-правовая система противодействия преступлениям в сфере компьютерной информации практически интегрирована в систему конвенции[3].

Уважая представленные точки зрения, тем не менее, следует констатировать, что если года два-три назад гипотетически можно было

2020. № 1; Протасевич А.А., Зверянская Л.П. Борьба с киберпреступностью как актуальная задача современной науки // Всероссийский криминологический журнал. 2011. № 3.

[1] Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#s6sltZT8ojzV24w91 (дата обращения: 20.04.2023 г.).

[2] Мирошников Б.Н. Перспективы международного сотрудничества в рамках Конвенции о киберпреступности // Национальные интересы: приоритеты и безопасность. 2007. № 6. С. 47.

[3] Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использование информационно-коммуникационных технологий: учеб. пособие. М.: ИНФРА-М, 2018. С. 18.

рассматривать данную конвенцию как потенциальный вариант ратификации при условии исключения п. «b» ст. 32, то в условиях нынешней внешнеполитической тенденции и деструктивных отношений с европейскими государствами и США подписывать континентальный международный акт, ограничивающий информационный суверенитет государства, нельзя.

Альтернативой ему являются два вариативных пути. Первый заключается в развитии и совершенствовании Соглашения о сотрудничестве в области обеспечения международной информационной безопасности в рамках Шанхайской организации сотрудничества от 16 июня 2009 г.[1]

Итогом принятия Соглашения стало официальное международно-правовое закрепление «основных понятий в области обеспечения международной информационной безопасности», среди которых особо выделяются «информационная война», «информационное оружие», «информационная преступность», «информационный терроризм», «информационное пространство» и т.д.[2]

Так, понятие «информационная война» предлагается определять следующим образом – это противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны[3].

«Информационное пространство» – сфера деятельности, связанная

---

[1] Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (вместе с «Перечнями основных понятий и видов угроз, их источников и признаков») (заключено в г. Екатеринбурге 16 июня 2009 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=51984#Kf6mtZTeqMca dQ9Z1 (дата обращения: 20.04.2023 г.).

[2] Там же.

[3] Там же.

с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе, на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию[1].

В приложении 2, принятом в качестве дополнения к Соглашению, излагается подробный перечень информационных преступлений, таких как:

– незаконное проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации;

– умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ;

– осуществление DDoS-атак (отказ в обслуживании) и иных негативных воздействий;

– причинение ущерба информационным ресурсам;

– нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни;

– использование информационных ресурсов и методов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т. д.

Следует отметить, что практически каждый из представленных примеров информационной преступности в российском уголовном праве криминализован, за исключением разве что проведения DdoS-атак как обособленного и самостоятельного состава преступления. Да, количество стран-участниц Шанхайского Соглашения несколько меньше, чем Будапештского, но, тем не менее, по численности населения эти страны представляют большую половину жителей земли, а следовательно,

[1] Там же.

и непосредственных субъектов информационных правоотношений. Из минусов и недостатков Шанхайского соглашения следует отметить отсутствие четко сформулированных составов преступлений, классификации информационных преступлений по направлениям и т.д.

В отечественном научном дискурсе в настоящий момент сталкиваются две ключевые позиции относительно международно-правовых аспектов обеспечения информационной безопасности в контексте терминологии. Российское законодательство, ряд гуманитарных наук, таких как политология, социология, юридические науки (в том числе уголовное право) в целом стоят на позициях использования всеобъемлющего понятия – «международная информационная безопасность», которое охватывает не только правовые и технические, но и политические, экономические и социальные аспекты, в том числе акцентируя внимание на политико-идеологических угрозах информационной безопасности (использования информационных атак, хакерских атак как элементов внешнеполитической деятельности против суверенных государств). Европейская и американская научная концепция апеллирует к понятию «кибербезопасность», делая акцент на техническом обеспечении информационной безопасности[1].

Вторая позиция, основанная на западном определении киберпреступности, логически восходит к науке кибернетике – науке, посвященной общим законам получения, хранения, передачи и преобразования информации в сложных управляющих системах[2]. Дефиниции «киберпространство», «кибербезопасность», «киберпреступления» выступают частными случаями отдельного института преступлений в сфере компьютерной информации и виртуальной реальности, однако информационная безопасность, в том числе международная

[1] См.: Крутских А.В., Зиновьева Е.С. Международная информационная безопасность: подходы России. М.: МГИМО, 2021. С. 34.

[2] Глушков В.М., Амосов Н.М., Артеменко И.А. Энциклопедия кибернетики. Киев: Главная редакция украинской советской энциклопедии, 1974. С. 440.

информационная безопасность, толкуется гораздо шире, с включением преступных деяний, связанных с информацией в любых формах ее материальной и нематериальной действительности. Следовательно, определение информационного пространства, равно как и информационной безопасности, будет более общим и широким определением для киберпространства и кибербезопасности соответственно.

Продолжая развивать тему эволюции международно-правового регулирования информационной безопасности, нельзя не отметить несколько Резолюций Генеральной Ассамблеи ООН, которые хоть и носят рекомендательный характер декларативного обобщения мнений суверенных государств, тем не менее, отражают их общий концептуальный взгляд на дальнейшее развитие обсуждаемого вопроса. Так, резолюция ГА ООН 2013[1] г. 68/167 «Право на неприкосновенность личной жизни в цифровой век» впервые публично подтверждает и уравнивает информационные права человека в офлайн пространстве и в киберпространстве.

В настоящий момент – это все крупные международные акты, посвященные информационной безопасности и борьбе с информационной преступностью. Очевидно, что пока на уровне главной международной организации – ООН – не будет принята Всеобъемлющая конвенция об обеспечении информационной безопасности, проблема не разрешится. Данную позицию публично занимает Российская Федерация, на всех площадках продвигая свой проект, разработанный в 2011 г. Конвенция «Об обеспечении международной информационной безопасности» могла бы унифицировать подходы национальных уголовно-правовых систем к ключевым проблемам противодействия информационной преступности, наладить тесное взаимодействие на уровне Интерпола, организовать систему взаимного поиска лиц, совершающих преступления в киберпространстве,

[1] Право на неприкосновенность личной жизни в цифровой век: Резолюция, принятая Генеральной Ассамблеей 18 декабря 2013 г. A/68/456/Add.2 // Официальный сайт ООН. URL: https://www.un.org/ru/ga/third/68/third_res.shtml (дата обращения: 22.02.2023 г.).

в том числе путем определения истинного IP адреса устройства, с которого совершались преступления[1].

В 2021 г. Российская Федерация внесла еще один проект Конвенции «О противодействии использованию информационно-коммуникационных технологий в преступных целях», содержащий ряд важных определений, таких как вредоносная компьютерная программа, информация, информационно-коммуникационные сети, компьютерная атака, объекты критической инфраструктуры и т.д. В нем предлагается универсальная криминализация целого ряда преступлений, в том числе таких, которые не содержатся в действующей редакции УК РФ, а именно[2]:

– нарушение функционирования информационно-коммуникационных сетей;

– неправомерное воздействие на цифровую информацию;

– неправомерный перехват;

– создание и использование цифровой информации для введения пользователя в заблуждение (умышленное противоправное создание и использование цифровой информации, сходной до степени смешения с уже известной пользователю и вызывающей доверие информацией, повлекшее причинение существенного ущерба).

В перспективе было бы интересно оценить возможную имплементацию предлагаемых норм в систему отечественного уголовного права, так как ранее уже отмечалось, что положения гл. 28 УК РФ требуют не косметического ремонта, а существенной переработки.

Еще одним позитивным положением, содержащемся в названной

---

[1] Лихачев Н.А. Международное уголовно-правовое противодействие преступлениям в сфере информационной безопасности // Вопросы российского и международного права 2023. № 4. С. 439.

[2] Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях: проект от 29.06.2021 г. // Официальный сайт ООН. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf (дата обращения: 22.02.2023 г.).

Конвенции, выступает закрепление возможности и необходимости государств-подписантов обмениваться компьютерной информацией, помогающей в совместном расследовании трансграничных преступлений против информационной безопасности. Связано это с тем, что практика раскрытия и расследования преступлений в сфере компьютерной информации невысока, и в первую очередь это связано с проблемой установления лица, подозреваемого в совершении преступления. В настоящее время развитие компьютерных технологий достигло уровня, позволяющего злоумышленнику эффективным образом скрывать электронные следы своего преступления, используя технологии VPN, блуждающего IP, путем подмены его иностранными данными, а в некоторых случая и электронными следами нескольких стран. Государства же, как правило, не предоставляют даже по официальным запросам данные относительно владельца IP-адреса, что препятствует расследованию уголовного дела.

Решение данной проблемы могло бы заключаться в принятии такой всеобъемлющей Конвенции на уровне ООН, а также создании впоследствии на ее базе международной организации со справедливым и равным представительством государств-подписантов. Задачей этой организации являлось бы формирование единой универсальной системы доменных имен (IP-адресов) и последующего контроля над ней. Это позволило бы при расследовании преступлений определять юрисдикцию и в двухстороннем порядке обмениваться данными о предполагаемом преступнике.

Проблема международно-правового, в том числе уголовно-правового, регулирования общественных отношений в сфере обеспечения обмена информации в ИТС «Интернет», поддержания функционирования ТСПУ остается актуальной. Единого универсального регулирующего их акта или международного договора на данный момент не принято. Не разработан подобный договор и на более узком – региональном – уровне. В рамках Содружества Независимых Государств (далее – СНГ) не принята ни дорожная карта, ни проект контроля функционирования ТСПУ, хотя в отечественном

уголовном законе уже появились нормы-новеллы, предусматривающие ответственность за преступные деяния в данной сфере (ст. 274^2 УК РФ).

Обращаясь к нормативно-правовым актам стран ближнего зарубежья, следует заметить, что интерес представляют положения ст. 278^1 и 278^7 УК Республики Узбекистан, предусматривающих уголовную ответственность за создание, внедрение и эксплуатацию информационных систем, причинивших вред в том числе государственным интересам, и незаконный доступ к сетям телекоммуникаций с целью пропуска международного трафика в обход систем защиты соответственно[1].

В данном ракурсе исследовательский интерес представляет вступившая в силу 20 декабря 2018 г. Директива (ЕС) 2018/1972 Европейского парламента и Совета от 11 декабря 2018 г. о Европейском кодексе электронных коммуникаций[2]. Согласно новым правилам риски, связанные с обеспечением безопасности сетей связи ИТС «Интернет», квалицированным оказанием соответствующих услуг, возлагаются в государствах-подписантах на непосредственных поставщиков. Видится закономерным, что нарушение подобных правил может стать основанием для уголовной ответственности и последующей криминализации соответствующих неправомерных деяний в данной сфере. Специально созданное, в том числе для подобных целей, Агентство Европейского союза по сетевой и информационной безопасности (ENISA) призвано координировать и реализовывать принятые положения государствами-членами с целью более эффективной и универсальной рецепции норм в национальные правовые системы. Таким образом, очевидно, что европейский законодатель стремится создать единую архитектуру

[1] Уголовный кодекс Республики Узбекистан 1994 г. (ред. от 21 февраля 2024 г.). URL: https://online.zakon.kz/Document/?doc_id=30421110 (дата обращения: 22.02.2024).

[2] См.: Директива Европейского Парламента и Совета Европейского Союза 2018/1972 от 11 декабря 2018 г. об установлении Европейского Кодекса электронных коммуникаций (новая редакция) // ИПС «ГАРАНТ». URL: https://base.garant.ru/72944624/?ysclid=luqu05cqc9351432827. *Директива адресована государствам – членам Европейского Союза. Российская Федерация членом ЕС не является*.

правового обеспечения информационной безопасности, в том числе и в уголовно-правовой сегменте. Отдельно прописывается необходимость оперативного уведомления компетентных государственных органов о возникших реальных рисках и угрозах безопасности компьютерных сетей.

Вопрос же международно-правового реагирования на преступления подобного рода, межгосударственного взаимодействия правоохранительных органов в соответствующей сфере остается нерешенным. Возможно, в целях более эффективного расследования и привлечения лиц к уголовной ответственности следует подумать об универсальных нормах уголовного законодательства на наднациональном уровне.

Связано это с проблемами кибероперациий, направленных на прямое воздействие на критические объекты информационной инфраструктуры, что способно вывести из строя работу крупных предприятий, заводов и НПЗ посредством отключения их компьютерных сетей и систем. Кибероперации становятся новой формой агрессии, угрожая безопасности не только прав и свобод отдельных лиц и социальных групп, но и целых государств и государственных военно-политических блоков. Одним из экспертных актов международного уровня стало «Таллиннское руководство по международному праву, применимое к кибервойне». Этот документ представляет собой аналитический академический акт, осмысливающий нормы международного права, нормы права вооруженных конфликтов и международного гуманитарного права относительно кибератак и кибервойн.

Таллиннское руководство было одной из первых попыток провести рассмотрение феномена кибероперациий и кибервойн посредством комплексного анализа различных трактовок и позиций в юридической науке и практике с опорой, в первую очередь, на нормы международного права[1].

Важным выводом является относимость принципов международного права к ведению кибервойн и проведению кибератак. Законы и правила

[1] Тимошков С.Г. Кибератака как современная форма совершения акта агрессии // Вестник РГГУ. Серия «Экономика. Управление. Право». 2017. № 1 (7). С. 132.

ведения войны, в том числе нормы, предусматривающие уголовную ответственность на международном уровне за нарушение правил ведения войны, должны быть применимы и к информационному противоборству.

В то же время важно понимать, что традиционные правила jus ad bellum и jus in bello не применимы к современному ведению борьбы в информационной сфере. В первую очередь это связано с деградацией принципов территориальности, возможностью опосредованного воздействия на объект из пределов другой юрисдикции, невозможностью установления источника воздействия априори и т.д.

В данном руководстве сказано: «Важно отметить, что данный документ не является руководством по вопросам «кибербезопасности», исходя из общего понимания данного термина. Кибершпионаж, кража интеллектуальной собственности и другие виды киберпреступлений представляют собой серьезную угрозу для всех государств, в том числе и для корпораций, и для частных лиц. Адекватные меры по противодействию подобным видам преступлений должны быть предприняты и на национальном уровне, и на международном. Соответственно, данное Руководство не содержит прямых указаний, которые должны быть выполнены в целях предотвращения киберпреступлений, лишь рекомендации по развитию норм международного права, поскольку существующие нормы по разрешению конфликтов в реальном мире не могут быть применимы для разрешения конфликтов в киберпространстве»[1].

Важным диалектическим вопросом на уровне международного уголовного права является квалификация кибератак и информационных операций. Является ли целенаправленное воздействие на объекты критической информационной инфраструктуры государства актом агрессии и casus belli и порождает право государства на оборону или нет? Какой объем и характер последствий проведения операций подобного рода достаточен

[1] Schmitt M.N. Op. cit. P. 7-10.

для определения их как вооруженного нападения? Каков механизм совместного расследования и последующего привлечения к уголовной ответственности лиц, причастных к подобной преступной деятельности? Следует ли относить лиц, состоящих на государственной службе или же на возмездной основе осуществляющих кибератаки и информационные операции, к комбатантам, на которых не распространяются нормы уголовного законодательства? Могут ли компьютерные сети гражданского назначения быть легитимными военными целями, в том числе блокирование здравоохранения, промышленности, энергетики и иных объектов жизнеобеспечения общества?

Отдельного внимание заслуживают вопросы квалификации киберсаботажа в космосе – блокирования или иного целенаправленного воздействия на государственные спутники в целях нарушения их базового функционирования.

На международном уровне проблемы уголовно-правового регулирования обеспечения информационной безопасности связаны со следующими факторами:

– исчерпывающим определением круга лиц, причастных к совершению преступления и привлекаемых впоследствии к уголовной ответственности;

– процессом доказывания, в том числе собиранием доказательств, оценкой их допустимости и достоверности;

– тем, что квалификация кибератак затрудняется определением целей и мотивов, а также направленности умышленного воздействия лиц;

– определением конечного организатора и распределения ролей на всех стадия совершения преступления, представляющих большую сложность.

Массовый характер совершения преступлений против информационной безопасности лишний раз свидетельствует о необходимости универсализации международно-правовой нормативной базы, а после этого и национального уголовного законодательства, обмена опытом расследования подобных

преступлений и совместной координации противодействия.

Несмотря на наличие уже принятых международно-правовых актов в сфере обеспечения информационной безопасности, их практическая значимость относительно невелика. На сегодняшний день в мире нет универсального определения понятия преступлений против информационной безопасности, нет четкого перечня составов соответствующих преступлений и их классификации. Бесспорно, следует отметить положительную роль Будапештского и Шанхайского актов, однако они являются актами континентального, но никак не всеобъемлющего уровня. К тому же они обладают силой акта «мягкого права» и выражают в большей степени лишь политическую волю и позиции государств-подписантов. Международному сообществу только лишь предстоит создать единую систему обеспечения информационной безопасности. В большей степени успешность подобных действий зависит от политической воли, желания и договоренности великих держав, возможности нахождения между ними приемлемого консенсуса.

Определение информационной войны, официально принятое ШОС, предусматривает ряд составов преступлений, предусмотренных УК РФ, что позволяет относить данный термин к уголовно-правовой науке. Однако в настоящий момент дефиниция «информационная война», разработанная в политологии, философии, филологии и ряде гуманитарных наук, не имеет представительства в уголовно-правовой науке.

Современное понимание прав и свобод человека и гражданина на международном уровне заключается в закреплении приоритетной субъектности индивида в обеспечении свободы слова и неприкосновенности частной жизни. В то же время важно понимать, что нельзя абсолютизировать свободу слова, свободу собирания и распространения информации, так как это неизбежно приведет к нарушению прав других субъектов. Определено, что государство на международном уровне несет моральную, политическую, а в отдельных случаях и юридическую ответственность

за совершение гражданами преступлений в сфере информационной безопасности. Следовательно, главной задачей государственных институтов является обеспечение контроля за распространением информации, особенно ограниченной или социально опасной.

Очевидно, что на международном уровне право субъекта на информацию существенным образом трансформируется. Имеет место запрос на принятие всеобъемлющей Хартии информационных прав с уклоном на цифровой аспект, а также специфику проведения информационных операций. Итак, в настоящее время на международном уровне происходит активное формирование будущей архитектуры правового обеспечения информационной безопасности. Уголовно-правовые аспекты в данном случае играют ключевую роль, ибо количество информационных операций и кибератак растет в геометрической прогрессии, они становятся более разнонаправленными, их классификация усложняется. Отсутствие единого международного договора, определяющего кибератаки, механизм уголовно-правового противодействия им и установления ответственности позволяет использовать их в качестве инструмента политического воздействия.

1.4 Обеспечение информационной безопасности в зарубежном уголовном праве

Проблема обеспечения информационной безопасности не является уникальной и индивидуальной проблемой для России. Как уже отмечалось, это универсальная проблема, касающаяся практически всех развитых и развивающихся государств. Процессы глобализации позволили интегрировать в международные процессы все государства и общественные институты. При этом специфика нормативно-правового регулирования информационной безопасности, особенно ответственности за преступления в сфере компьютерной информации и административно-правового реагирования на

них может существенно отличаться от привычной российской практики.

Проблеме исследования зарубежных аспектов обеспечения информационной безопасности в отечественной уголовно-правовой науке уделено немалое внимание. В разные годы к этой проблеме обращались такие ученые, как Р.И. Дремлюга, А.И. Коробеев[1], В.А. Мазуров, А.В. Пелевина[2], Д.П. Потапов, В.В. Сорокин[3].

По данным ООН, к концу 2021 г. число пользователей сети «Интернет» составило более 4,9 млрд человек[4]. Очевидно, что это число за последний год выросло, только в КНР в 2021 г. число пользователей «Интернета» достигло более 1 млрд человек (рост за год – 42,96 млн человек)[5].

Передовыми зарубежными государствами, чьи уголовно-правовые системы противодействия преступлениям в сфере обеспечения информационной безопасности являются одними из лучших, традиционно признаются США и КНР. В связи с этим будет представлен анализ уголовного законодательства этих стран, дополнительно внимание будет уделено уголовным законам Франции и Германии.

Правовое регулирование функционирования сети «Интернет» в Китае сильно отличается от его осуществления в рамках привычной отечественной или европейской системы. Оно характеризуется крайне высокой степенью государственно-правового регулирования, административно-правового и уголовно-правового контроля за частной жизнью пользователей в сети.

---

[1] См.: Дремлюга Р.И. Критическая информационная инфраструктура как предмет посягательства в законодательстве зарубежных стран // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 3. С. 27-36; Дремлюга Р.И., Коробеев А.И. Ответственность за создание, использование и распространение вредоносных компьютерных программ по законодательству зарубежных стран // Российский следователь. 2022. № 5. С. 67-71.

[2] Пелевина А.В. Ответственность за компьютерные преступления в романо-германской правовой системе // Пробелы в российском законодательстве. 2016. № 3. С. 77.

[3] Мазуров В.А., Потапов Д.П., Сорокин В.В. Компьютерные преступления: анализ уголовного законодательства США и Германии // Известия АлтГУ. 2005. № 2. С. 62.

[4] 37 процентов людей никогда не пользовались интернетом. Новости // ООН. URL//https://news.un.org/ru/story/2021/11/1414732 (дата обращения: 10.02.2023 г.).

[5] Число пользователей интернета в Китае к концу 2021 года превысило 1 млрд человек // ТАСС. URL: https://tass.ru/obschestvo/13855855 (дата обращения: 10.02.2023 г.).

Впервые сеть «Интернет» появилась в КНР в 1987 г. В Пекинском институте физики и высоких энергий профессор Цянь Тяньбай в рамках проекта CANET (Chinese Academic Network) отправил первое электронное письмо из материкового Китая[1].

Я.В. Лексютина отмечает, что система контроля и регулирования сети «Интернет» в КНР носит комплексный многоаспектный характер. В ней можно выделить несколько направлений[2]:

– дифференциация материалов с использованием специального программного обеспечения и технических методов;

– контроль за материалами представителями государственной цензуры;

– создание системы нормативно-правового регулирования и контроля за сетью «Интернет».

Китайское уголовное законодательство прошло несколько этапов от своего становления и развития до актуального уровня уголовно-правового регулирования. Первые нормы о преступлениях в сфере компьютерной информации были введены в УК КНР приблизительно в один период с УК РФ (в 1997 г.). В отличие от российского законодательства, нормы уголовного законодательства КНР не имеют персонифицированного названия, только порядковый номер, они будут идентифицироваться согласно непосредственному деянию[3]:

– публичное оскорбление другого человека с применением насилия или иных способов либо фальсификация фактов в целях очернения другого человека при отягчающих обстоятельствах (ст. 246);

– вторжение в компьютерные информационные системы

[1] Вильданов Р.Р., Кутушева Э.Н. Система государственного регулирования интернета в Китайской Народной Республике // Вестник УГНТУ. Наука, образование, экономика. Серия: Экономика. 2021. № 3 (37). С. 116.

[2] Лексютина Я.В. Политика китайского руководства в вопросах контроля и регулирования Интернета // Общество и государство в Китае. 2015. № 1. С. 206.

[3] Уголовный кодекс Китая / под ред. А.И. Коробеева и А.И. Чучаева, пер. с кит. Хуан Даосю. М., 2017. С. 133.

государственного значения (ст. 285);

– разрушение компьютерных информационных систем (ст. 286.3);

– финансовое мошенничество, кража, коррупция, использование не по назначению общественных средств, похищение государственной тайны или другие преступления, совершенные при помощи компьютера (ст. 287).

Данные статьи направлены на обеспечение безопасности и защиты использования компьютерных и информационных систем, в том числе в таких ключевых сферах, как национальная оборона, наука, государственное устройство. Они содержатся в гл. 6 «Преступления против порядка управления и общественного порядка», что подчеркивает высокую степень их общественной опасности и угрозы для китайского общества и государства.

Анализируя конкретные нормы, стоит заметить, что диспозиция ст. 286 УК КНР, наравне с используемой в российском уголовном законодательстве «модификацией», содержит такие признаки, как «дополнение» и «создание помех», а также «исправление». На наш взгляд, такой подход представляется интересным, так как позволяет упростить квалификацию и понимание уголовно-правовой нормы, определяя действия преступного лица конкретными формулировками.

Еще одним примером отличия практики конструирования уголовно-правовых норм в УК КНР и УК РФ является ст. 287, которая предусматривает объединение в рамках одной диспозиции традиционных составов преступлений (мошенничества, дачи взятки и т.д.), но с применением компьютерных технологий. Отечественный законодатель пошел по пути криминализации подобного рода деяний, добавляя их к уже имеющимся составам преступления в качестве квалифицирующих признаков. Подобных составов в УК РФ насчитывается более 20.

Статья 246 УК КНР предусматривает уголовную ответственность за публичное оскорбление другого лица или осуществление действий по фальсификации фактов в целях очернения этого лица, в том числе через

информационные сети. Как известно, УК РФ содержит ст. 319 «Оскорбление представителя власти», однако квалифицирующего признака в диспозиции уголовно-правовой нормы, связанного с совершением деяния в сети «Интернет», не предусмотрено. Ранняя редакция УК РФ предусматривала отчасти схожий с предусмотренным в китайской уголовно-правовой норме состав преступления в ст. 130 «Оскорбление», который выражался в унижении чести и достоинства лица, совершенном в неприличной форме, а квалифицирующим признаком было оскорбление в публичной форме или в средствах массовой информации. Данное деяние было декриминализовано в 2011 г. Полагаем, что это было правильное решение законодателя, так как степень общественной опасности подобного рода деяний минимальна, это сфера гражданско-правовых отношений[1].

Что касается доктринальной базы, то китайская уголовно-правовая наука оперирует понятием киберпреступлений, о чем пишет Ван Гуанлун, который понимает под киберпреступлениями посягательства против компьютерных сетей, безопасности электронных данных, совершаемых с помощью интернет-технологий в виртуальном пространстве (киберпространстве)[2]. Представляет интерес китайское философское уголовно-правовое учение о месте преступления, характеризуемом, в том числе, киберпространством. Юй Чжиган полагает, что в настоящий момент общество вступило в фазу существования в двумерном пространстве, одно из которого – это привычная реальность, а второе – онлайн-общество в сети «Интернет»[3].

Ключевой системой, обеспечивающей контроль за данными

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07 декабря 2011 № 420-ФЗ (последняя редакция) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_122864/ (дата обращения: 22.02.2023 г.).

[2] Ван Гуанлун. Уголовно-правовое регулирование противодействия киберпреступности в Китае: состояние, тенденции, недостатки // Вестник СПбГУ. Серия 14. Право. 2022. № 3. С. 662-663.

[3] Yu Zhigang. 2010a. Cybercrime and China’s Criminal Law response // Zhongguo Shehuikexue 3: P. 109-126.

и информацией в сети «Интернет» в КНР, является «Золотой щит», запущенный 1998 г. как тестовый проект и к 2006 г. обеспечивший государству полный контроль над сетью. Этот электронный барьер осуществляет предоставление доступа физическим и юридическим лицам, а также осуществляет блокировку Интернет-ресурсов, которые представляют угрозу безопасности государства, в частности проявления кибертерроризма, еще одного актуального и нового направления в уголовно-правовой теории и практике[1]. Более того, информационные платформы, предоставляющие в КНР доступ в сеть, возможность осуществления обмена информацией, в том числе и социальные сети, несут непосредственную юридическую ответственность за сведения, которые будут распространены посредством этой платформы.

Понятие кибертерроризма является продуктом американской уголовно-правовой науки. Оно было сформировано в середине 1980 г. Б. Коллиным, определившим его как использование высоких технологий в целях парализации работы ключевых объектов национальной инфраструктуры, запугивания правительства и гражданского населения[2].

В КНР принято несколько норм, устанавливающих ответственность за проявления кибертерроризма. Например, ст. 291.1 УК КНР предусматривает распространение заведомо ложной информации о биохимической или радиоактивной опасности, а также заведомо ложной террористической информации.

По данным китайских исследователей, КНР уже несколько лет занимает высокие позиции среди государств, массово подвергающихся кибератакам. Ряд ученых выступает за организацию международного уголовно-правового сотрудничества с целью координации и определения мест совершения преступлений в сфере компьютерной информации. Существенной проблемой

[1] Navarria G. China: the Party, the Internet, and power as shared weakness // Global Change, Peace and Security. 2016. Vol. 29. P. 1-20.

[2] Collin B.C. The Future of Cyber Terrorism // Crime & Justice International. 1997. Vol. 13, no. 2. March. P. 15-18.

является определение местонахождения лица, совершившего преступление, если источник находится вне пределов юрисдикции государства-потерпевшего. При этом злоумышленниками нередко в промежуточных целях сокрытия следов преступления используются промежуточные доменные адреса, указывавшие на его местоположение в любом условном государстве, в котором де-факто они не находятся[1].

Таким образом, КНР в публичном, правовом и политическом поле поддерживает предложения Российской Федерации по принятию всеобъемлющей конвенции по международной информационной безопасности. Краткий анализ уголовно-правовой практики КНР позволяет сделать вывод о схожести уголовно-правовых проблем и информационных угроз в правовом пространстве Российской Федерации и Китайской Народной Республики. Однако степень контроля за информационным пространством, практика суверенизации «Интернета» в КНР существенно выше, чем у нас. Представляется, что, говоря о зарубежном опыте противодействия преступлениям против информационной безопасности в контексте отечественной уголовной политики, следует сделать вывод о важности выбора путей повышения уровня самосознания граждан, их ответственности за правомерное поведение, осознания принципа неотвратимости наказания и повышения уровня информационной грамотности населения, что безусловно снизит уровень преступности.

Возвращаясь к теме проявления, сущности и понятия кибертерроризма и киберпреступности, нельзя не обратиться к зарубежному опыту обеспечения информационной безопасности в США. Американская уголовно-правовая доктрина обращает большое внимание на вопросы противодействия кибертерроризму.

Так, Д. Дэннинг полагает, что кибертерроризм – это осуществление противозаконных компьютерных атак на государственные информационные

[1] Seung Hyun Kim, Qiu-Hong Wang, Johannes B. Ullrich. A comparative study of cyberattacks // Communications of the ACM. 2012. Vol. 55, iss. 3. P. 66-73.

системы для запугивания или понуждения правительства или общества к совершению определенных действий и достижения преступных целей политического или социального характера. Киберпространство автор понимает как средство совершения террористической атаки, нарушающей неприкосновенность цифровой собственности[1].

Вальтер Лакер – историк и американский исследователь терроризма – писал, что электронный век сделал кибертерроризм возможным. Когда-то опора науки – фантастика, машина судного дня – сегодня вырисовывается как реальная опасность. Сочетание технологий и терроризма создают неопределенное и пугающее будущее[2].

Мора Конвей приводит классификацию правомерных и неправомерных (уголовно-наказуемых) деяний в сети «Интернет»[3]:

– правомерное использование интернета в целях общения, коммуникаций, выражения идей и связи с интернет-пользователями, использование электронной почты, чтения новостей и т.д.;

– неправомерное использование сети «Интернет»: нарушение неприкосновенности информационных ресурсов, взломы веб-сайтов или информационной инфраструктуры, хакерство и хакерский активизм, осуществление DDoS-атак;

– оскорбительное использование – использование сети «Интернет» в целях повреждения компьютерной информации, взлома с последующей кражей персональных данных (например, данных кредитной карты);

– кибертерроризм – умышленная атака, совершаемая террористами через сеть «Интернет», приводящая к насилию над потерпевшим или серьезному экономическому ущербу, например, использование сети

[1] Denning D.E. A View of Cyberterrorism Five Years Later // Internet Security: Hacking, Counterhacking, and Society / ed. by K. Himma. Sudbury, MA, 2006. P. 123-141.

[2] Walter Laqueur. The New Terrorism: Fanaticism and the Arms of Mass Destruction. Oxford: Oxford University Press, 1999. P. 254.

[3] Cyberterrorism: Hype and Reality Maura Conway Dublin City University. 2007. URL: https://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf (дата обращения: 22.02.2023 г.).

«Интернет» для нападения на информационные сети Нью-Йоркской фондовой биржи.

В США на протяжении нескольких десятилетий действует Закон «Об управлении информационной безопасностью»[1] как один из разделов Закона «Об электронном правительстве»[2], направленный на обеспечение доступа общества к государственно-значимой информации и сведениям. Он в разделе 5 содержит еще один Закон – «О защите конфиденциальной информации и статистической эффективности («CIPSEA»)[3]. Закон устанавливает единые меры защиты конфиденциальности информации, собираемой статистическими центрами США для статистических целей.

Согласно этому закону, под информационной безопасностью в США принято считать:

– обеспечение безопасности информации и информационных систем от осуществления не санкционируемого доступа, использования, раскрытия, распространения, модификации или уничтожения информации;

– обеспечение целостности информации и информационных ресурсов от осуществления неправомерного изменения или уничтожения, в том числе гарантии ее подлинности;

– обеспечение непрерывной конфиденциальности информации, что понимается как поддержание ограничения к ее доступу, невозможность распространения информации, в том числе информации о частности жизни и собственности лица.

Отметим, что наравне с используемыми в отечественном уголовном

---

[1] Закон об электронном правительстве США. Раздел 3. Информационная безопасность. 2002. URL: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf (дата обращения: 19.03.2023 г.).

[2] Закон об электронном правительстве США. 2002. URL: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf (дата обращения: 19.03.2023 г.).

[3] Закон об электронном правительстве США. Раздел V. Конфиденциальная информация защита и статистическая эффективность. 2002. URL: https://georgewbush-whitehouse.archives.gov/omb/inforeg/cipsea/cipsea_statute.pdf (дата обращения: 19.03.2023 г.).

законодательстве критериев неправомерного воздействия на информацию и информационные ресурсы в США дополнительно применяется такой критерий, как «раскрытие» информации, которая носила конфиденциальный характер.

В российской уголовно-правовой науке проблеме кибертерроризма тоже уделяется существенное внимание. Можно выделить работы Е.А. Капитоновой, Г.П. Кулешовой, Г.Б. Романовского[1], О.А. Степанова[2], Е.М. Якимова[3]. Тем не менее, на официально-правовом уровне понятийно-категориальный аппарат, основанный на использовании корня «кибер», не прижился. В отечественной практике доминирует тенденция использования парадигмы «преступления против информационной безопасности», «преступления в сфере компьютерной информации» и т.д.

В уголовном законодательстве стран постсоветского пространства также уделяется внимание преступлениям против информационной безопасности. Так, криминализация собственно киберправонарушений в уголовных кодексов государств – участников СНГ осуществлена:

– в гл. 7 «Уголовные правонарушения в сфере информатизации и связи» (ст. 205-213) УК Казахстана 2014 г.;

– в гл. 30 «Киберпреступления» (ст. 272-273) УК Азербайджана 1999 г.;

– в гл. 31 «Преступления против информационной безопасности» (ст. 349-355) УК Республики Беларусь 1999 г.;

– в гл. 28 «Преступления против информационной безопасности» (ст. 298-304) УК Таджикистана 1998 г.;

---

[1] Кулешова Г. П., Капитонова Е.А., Романовский Г.Б. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения // Всероссийский криминологический журнал. 2020. № 1. С. 158.

[2] Степанов О.А. Противодействие кибертерроризму в цифровую эпоху. монография. М.: Юрайт, 2020. С. 56.

[3] Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10, № 2. С. 369-378.

– в гл. XX-1 «Преступления в сфере информационных технологий» (ст. 278-1-278-7) УК Узбекистана 1994 г.

– в гл. 42 «Преступления против информационной безопасности» (ст. 304-306) УК Кыргызстана 2017 г. и в гл. 29 «Проступки против информационной безопасности» (ст. 159-160) Кодекса Кыргызстана о проступках 2017 г.;

– в гл. 33 «Преступления в сфере информатики и связи» (ст. 333-335.3) УК Туркменистана 1997 г.;

– в гл. XI (ст. 259-261-1) «Информационные преступления и преступления в области электросвязи» УК Молдовы 2002 г.

Комплексный анализ уголовных законодательств зарубежных государств в соответствующей их части позволяет указать на наличие общих закономерностей. Ключевая из них выражается в наличии универсального родового объекта преступлений в сфере информационной безопасности. Связано это в том числе с учетом общего Модельного УК стран – участниц СНГ.

В Германии 22 апреля 2021 г. был принят Telecommunications Modernization Act (TKMG). Кроме того, действует Telecommunications Telemedia Data Protection Act (TTDSG) – Закон о защите данных в телекоммуникациях Германии, который сопровождается новым техническим руководством по осуществлению установленных законом мер по мониторингу телекоммуникаций. Уголовная ответственность за деяния, криминализованные отечественным законодательством (ст. 274-274^2 УК РФ), не предусмотрена. В этой сфере законодательство ФРГ только вступает в фазу своего развития.

Уголовное законодательство ФРГ представлено широким спектром деяний, направленных против обеспечения информационной безопасности. Отметим, что в УК Германии интересующие нас составы распределены по главам Особенной части и не структурированы в рамках группы

информационных преступлений. Их содержит, в частности, раздел 15, посвященный посягательствам на неприкосновенность частной жизни и частной тайны[1]. Особый интерес представляет ст. 201 кодекса, предусматривающая ответственность за противоправную запись непубличных разговоров (речи), не предназначенной для третьих лиц. Ответственность также влечет воспроизведение данной речи третьим лицам, если это противоречит интересам потерпевшего.

Преступные посягательства, связанные с компьютерной информацией, указаны в ст. 202a, предусматривающей ответственность за противоправное получение доступа к данным, особо защищенным от неправомерного доступа, хранящимся на электронных или магнитных носителях.

Статья 202b УК предусматривает ответственность за перехват данных пользователей, то есть, когда лицо, используя специальные технические средства, добывает для себя или третьих лиц передаваемые электронным образом данные.

Особое место в уголовном законе ФРГ занимает ст. 202d, предусматривающая наказание за распространение данных, которые не являются общедоступными, полученных преступным путем с целью личного обогащения или корыстного интереса третьего лица. Следует отметить, что в отечественном уголовном законодательстве не предусмотрена уголовная ответственность за распространение компьютерной информации, полученной неправомерным путем.

Уголовное законодательство Франции в вопросах обеспечения информационной безопасности и защиты объектов критической информационной инфраструктуры в сравнении с ФРГ представляется более развитым. Так, в УК Франции в разд. 2 включена гл. 3 «Атаки на

[1] Уголовное уложение Федеративной Республики Германия – Strafgesetzbuch (StGB) (пер. П.В. Головненкова). URL: https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB-%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf (дата обращения: 19.11.2023).

автоматизированные системы обработки данных» (статьи с 323-1 по 323-8)[1].

Так, ст. 323-1 УК содержит указание на интересное деяние, которое в УК РФ не предусмотрено, а именно: «мошеннический доступ» к системам обработки данных. Таким образом, мошенничество являет не только форму хищения, но и характеризует способ совершения преступления как обязательный признак объективной стороны преступления, выраженный в получении доступа к искомому объекту посредством обмана или злоупотребления доверием. Криминализована также контрабанда – ввоз во Французскую Республику специального технического оборудования или программного обеспечения, которое может быть заведомо использовано в целях совершения преступлений против автоматизированных систем обработки данных во Франции. Законом предусмотрено два вида наказания – штраф и лишение свободы на срок до 3/5 лет в зависимости от наличия квалифицирующих признаков. Важно также отметить, что французский законодатель предусматривает умышленную форму вины для преступлений против объектов КИИ. Кроме того, предусмотрена ответственность за нарушение тайны переписки, личной и семейной жизни.

Корреспондирующим отечественному уголовно-правовому термину «объекты критической информационной инфраструктуры» в зарубежном уголовном законодательстве является понятие «критические компоненты телекоммуникаций». Последние используются в практике только после официальной сертификации и тестирования, то есть когда признаются легальными продуктами производства, имея соответствующую декларацию надежности.

Уголовное законодательство Великобритании, регламентирующее ответственность за совершение преступлений против информационной безопасности, тесно связано с базовыми национальными нормативно-

[1] Уголовный кодекс Французской Республики. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006149839/#LEGISCTA00000614939 (дата обращения: 19.11.2023).

правовыми актами. Так, в Великобритании 17 ноября 2021 г. был принят Закон о телекоммуникационной безопасности (Telecommunications (Security) Act 2021). Этим законом внесены изменения в Закон о связи 2003 г. В ходе исследования установлено, что наибольший интерес представляют положения ст. 105A, согласно которой операторы связи обязаны самостоятельно выявлять различные угрозы киберустойчивости технического характера и самостоятельно предпринимать различные меры, направленные не пресечение и предупреждение киберугроз. Таким образом, очевидно, что британская модель обеспечения уголовной безопасности следует тенденции синергии государственно-частного регулирования общественных отношений[1].

Данный довод подтверждается ст. 105B, согласно которой операторы связи обязаны исполнять любые предписания государственного органа, имеющего статус официального регулятора. Статья 105E возлагает на государство обязательства по разработке и утверждению специальных правил по регулированию киберустойчивости и противодействию киберугрозам.

Уголовная ответственность за преступления в сфере информационной безопасности в Великобритании предусмотрена специальным Законом о связи от 17 июля 2003 года, согласно ст. 404 которого в случае, если «преступление в соответствии с любым законодательным актом, к которому применяется этот раздел, совершено юридическим лицом и доказано, что оно было совершено с согласия или попустительства, или может быть связано с каким-либо пренебрежением со стороны директора, менеджера, секретаря или другого подобного должностного лица корпоративного органа, или лица, которое предполагало действовать в любом таком качестве», такое лицо подлежит привлечению к уголовной ответственности на основании решения суда[2].

---

[1] Закон о телекоммуникационной безопасности Великобритании от 17 ноября 2021 г. URL: https://www.legislation.gov.uk/ukpga/2021/31/introduction/enacted (дата обращения: 13.01.2024).

[2] Закон о связи Великобритании от 17 июля 2003 года. URL: https://www.legislation.gov.uk/ukpga/2003/21/section/404 (дата обращения: 13.01.2024).

В 2016 г. в Великобритании был принят специальный Закон «О следственных полномочиях» (The Investigatory Powers Act»), ст. 3 которого устанавливает уголовную ответственность за перехват сообщения в ходе его передачи через частную, общественную либо государственную телекоммуникационную систему связи и предусматривает наказание в виде штрафа или реального лишения свобода сроком до 2-х лет. Согласно ст. 4 указанного закона под перехватом понимается получение доступа к сообщению лицом, которое не являлось его отправителем или получателем и не имеет законного основания на доступ к указанной информации[1].

Законодатель Канады также придерживается тенденции регулирования деятельности операторов связи и ТПСУ. Так, 14 июня 2022 г. начался процесс принятия законопроекта (Bill C-26), направленного на внесение изменений в Закон о телекоммуникациях. Его целью является большее участие государства в регулировании деятельности объектов критической информационной инфраструктуры путем более предметного нормативно-правового регулирования. Вследствие этого государственные органы получают практически неограниченный контроль за деятельностью местных частных операторов связи, осуществление надзора за исполнением правил безопасности связи, возможность ограничения пользования услугами связи и т.д.

Анализ международно-правовых и зарубежных аспектов изучаемой проблематики позволил сделать несколько выводов:

– у большинства государств, принимающих активное участие в противодействии преступлениям в сфере информационной безопасности, сформирована серьезная уголовно-правовая база, основанная на нормах национального административного законодательства;

– в большинстве случаев криминализированы деяния, связанные

[1] Закон о следственных полномочиях Великобритании от 29 ноября 2016 г. URL: https://www.legislation.gov.uk/ukpga/2016/25/introduction (дата обращения: 13.01.2024).

с неправомерным доступом к охраняемой законом информации, неправомерным воздействием на объекты критической информационной инфраструктуры, информации сети и т.д.;

– как китайские, так и российские представители науки и практики в качестве ключевых проблем уголовной ответственности за преступления против информационной безопасности выделяют не проблемы квалификации, а проблемы раскрытия и расследования в контексте определения лица из-за трудностей с определением домена (IP);

– в связи со сказанным единственным решением подобной проблемы видится приложение консолидированных усилий по принятию на уровне ООН международной Всеобъемлющей конвенции по международной информационной безопасности;

– тенденция регионализации международных актов по противодействию преступлениям против информационной безопасности приведет к тому, что злоумышленники будут действовать из стран-не подписантов против целей, находящихся в странах-подписантах;

– в результате сравнительно-правового исследования зарубежного уголовного законодательства перспективной видится рецепция положений Уголовного кодекса ФРГ, касающихся ответственности за противоправную запись непубличных разговоров с последующей передачей ее третьим лицам, особенно если указанные действия повлекли за собой наступление тяжких последствий, а также за распространение сведений (в случае отечественного уголовного законодательства – компьютерной информации), полученных преступным путем; представляет также интерес использование «мошенничества» как способа совершения преступления, то есть установление ответственности за получение доступа к охраняемой законом информации посредством обмана и злоупотребления доверием.

Отметим, что с данным мнением, а именно с необходимостью криминализации записи непубличных разговоров с последующей передачей

ее третьим лицам, если указанные действия повлекли за собой наступление тяжких последствий, распространения компьютерной информации, полученной преступным путем, получения доступа к охраняемой законом информации посредством обмана и злоупотребления доверием согласилось большинство (76%) опрошенных следователей МВД России, СК РФ, судей федеральных судов общей юрисдикции[1].

Таким образом, доктринальное исследование зарубежного уголовно-правового опыта противодействия преступлениям в сфере информационной безопасности позволяет реципировать наиболее эффективные нормы национального уголовно права в целях их последующей интеграции в отечественную правовую систему.

[1] См. Приложение 2.

2 Современная уголовно-правовая политика России в сфере обеспечения информационной безопасности

2.1 Тенденции уголовно-правовой политики в сфере обеспечения информационной безопасности

Общественные отношения в начале XXI в. подвергаются крупнейшим за всю историю технологическим, социальным, коммуникативным и культурным изменениям. Информационное пространство вследствие повсеместного внедрения ИТС «Интернет» вышло за рамки ограниченного сегмента распространения данных на региональном или национальном уровне. Процессы коммуникации носят трансграничный и межнациональный характер, практически не имея барьеров и бюрократических нормативных препятствий.

Популяризация и массовое использование портативных электронных устройств, компьютеризация общества привели к изменению устоявшейся на протяжении нескольких веков системы создания, обмена, распространения и хранения информации. Цифровизация направлена на совершенствование структуры обработки, передачи, распространения, хранения, изменения и обеспечения конфиденциальности данных, что сильно сократило практику применения традиционных предшествующих агрегатов информации.

Для рядового пользователя персональное компьютерное электронное устройство стало аккумулятором всех жизненно важных сведений о нем – фактов биографии, персональных данных, фото/видео/аудиоматериалов, географии его перемещения, информации относящейся к личной, семейной и медицинской тайне, позволяющих получить доступ к его банковским счетам и прочему цифровому имуществу.

Таким образом, необходимо констатировать, что компьютеризация привела к массовой цифровизации сведений, относящихся к личной, семейной, банковской, медицинской и иным видам тайны, а электронные

устройства стали наиболее распространенными ее непосредственными носителями.

В результате общественный строй коренным образом изменился, сформировалась постиндустриальная система или информационное общество со следующими чертами:

– превалирующей ролью информационной инфраструктуры, а также информационных и телекоммуникационных систем в процессах управления обществом и его коммуникациях;

– наличием принципиально новых методов и форм действий в информационном пространстве;

– повсеместным внедрением электроники и персональных компьютеров;

– устареванием роли «традиционных» СМИ, появлением альтернативных агрегаторов информации и лидеров общественного мнения;

– формированием национального информационного законодательства, развитием правового механизма регулирования всех процессов, связанных с информацией и ее статусом;

– получением возможности воздействия на неограниченную аудиторию со стороны каждого субъекта коммуникационных процессов в ИТС «Интернет»;

– маргинализацией и деградацией коммуникационных процессов во всех сферах.

Отсюда следует рост социальной значимости информации, потребностей граждан в достоверных и объективных сведениях об окружающем мире, политических, экономических, социальных и иных процессах. Очевидно, что развитие информационного пространства, формирование глобального информационного общества привело к качественным и количественным изменениям преступности. Эти процессы сопровождаются криминализацией ряда деяний, которые раньше либо не

представляли общественной опасности, либо отсутствовали вовсе в социальной действительности.

Стремительно развивается практика информационного противоборства, направленная на проведение информационно-психологических операций, массовое манипулирование потребителями информации, публичную дискредитацию различных субъектов информационных отношений, распространение недостоверных или заведомо ложных сведений, оправдание и пропаганду терроризма, экстремизма, нацизма и т.д.

Информационное противоборство приобретает все более осознанный, систематизированный характер, определяется государствами как вероятное поле боевых действий и военных операций. Таким образом, информационное пространство становится вероятным местом совершения преступлений.

Изменения, происходящие в информационном пространстве, отмечаются на государственном уровне. Так, в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. констатируется, что информационные и коммуникационные технологии стали неотъемлемой частью всех управленческих сфер. Выделяются проблемы международно- и национально-правового регулирования и защиты государственного суверенитета в информационном пространстве[1]. Учитывая возросшую роль информации, встроившейся в систему общественных отношений, следует отметить, что указанная проблематика приоритетным образом относится к сфере уголовно-правового регулирования.

Таким образом, сформировалось несколько основных направлений криминализации общественных отношений – появление компьютерной или цифровой преступности (в сфере информатизации и связи) и деяний, связанных с распространением различных сведений и данных, где

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09 мая 2017 г. № 203 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_ 216363/. (дата обращения: 14.01.2023 г.).

информация может выступать в качестве орудия совершения преступления[1]. Последний вид имеет свою специфику – цифровой признак встроен в состав преступлений общеуголовной направленности, дополняя содержание его отдельных элементов.

Данную классификацию можно дополнить еще одной группой деяний, которая представлена в нормах уголовного законодательства зарубежных стран. В Российской Федерации проходят дискуссии относительно рецепции соответствующих положений и их последующей имплементации в отечественное уголовное законодательство. Речь, в частности, идет об уголовной ответственности за осуществление хранения и распространения недостоверной, социально опасной, ограниченной информации или информации, полученной преступным путем, а также сведений об организованной преступности[2].

Некоторые субъекты используют глубинный Интернет для сокрытия своих данных в целях совершения различных преступлений, что приводит в том числе к «диджитализации» преступности[3].

Исходя из представленных направлений криминализации, можно судить о разнообъектности преступлений в сфере информационной безопасности. Так, первая группа деликтов в настоящее время объединена нормами, предусмотренными гл. 28 УК РФ «Преступления в сфере компьютерной информации». Объектом посягательств в данном случае являются общественные отношения в сфере обеспечения информационной безопасности и цифрового суверенитета личности, общества и государства. Предметом преступлений может выступать информация, различные

---

[1] См. об этом также: Соловьев В.С. Криминологическая типология механизмов совершения преступлений с использованием информационно-телекоммуникационных технологий // Вестник Краснодарского университета МВД России. 2021. № 4 (54). С. 50-57.

[2] Артемов В.Ю., Власов И.С., Голованова Н.А. и др. Новые направления развития уголовного законодательства в зарубежных государствах: сравнительно-правовое исследование: монография. М.: ООО «Юридическая фирма «Контакт», 2019. С. 223.

[3] Куфлева В.Н., Литовченко А.И. Проблемы квалификации преступлений, связанных с использованием шифрования информации и обеспечением анонимности в сети интернет // Общество: политика, экономика, право. 2021. № 9 (98). С. 81.

компьютерные системы и программы, критическая информационная инфраструктура и специальные технические средства.

В доктрине все чаще анализируется новая правовая категория – киберпространство. Она определяется как виртуальная среда, которая становится местом совершения преступлений в сфере информационной безопасности. При этом данный термин не нашел в науке всеобщей поддержки, и в качестве альтернативы встречаются такие понятия, как «виртуальная среда», «информационное пространство», «виртуальная реальность»[1] и т.д.

Киберпространство и виртуальную реальность следует рассматривать как синонимичные, сходные, но не тождественные понятия и явления, продукты современных компьютерных технологий, создающих новый нематериальный мир. Традиционное учение о месте преступления как факультативном элементе объективной стороны описывает его с позиции объекта материальной действительности – конкретного участка земной поверхности, имеющего свои географические ориентиры и координаты[2]. Например, зона экологического бедствия (ч. 2 ст. 254 УК РФ) или исключительная экономическая зона РФ (ст. 253 УК РФ).

Виртуальная реальность представляет собой полную компьютерную симуляцию вымышленного нематериального мира, существующего в форме электронного кода и хранящегося на электронном носителе. У пользователя эта технология должна вызывать ощущение реальности, полного присутствия и доверия к окружающему пространству. Ее следует отличать от дополненной реальности, когда компьютерная технология берет за основу реальную материальную действительность и трансформирует ее в мнимую, изменяя в восприятии субъекта те или иные познаваемые в процессе взаимодействия

[1] Дремлюга Р.И., Крипакова А.В. Преступления в виртуальной реальности: миф или реальность? // Актуальные проблемы российского права. 2019. № 3 (100). С. 162.

[2] Российское уголовное право. Общая часть: учебник / под ред. В.П. Коняхина и М.Л. Прохоровой. М.: КОНТРАКТ, 2014. С. 199.

объекты.

Киберпространство – явление несколько более широкое, нежели виртуальная реальность, оно дополнительно включает все общественные отношения и продукты, возникшие или созданные в ИТС «Интернет», а также нематериальные предметы, созданные компьютерными технологиями. Появление киберпространства привело к возникновению новой сетевой культуры и контркультуры, изменению правосознания граждан, новых правонарушений и преступлений.

Проблематика правового регулирования киберпространства, в первую очередь, лежит в плоскости определения понятийно-категориального аппарата. В российском уголовном праве понятие киберпространства официально не закреплено, а в научном сообществе единое мнение не сформировано. Некоторые ученые придерживаются позиции, согласно которой киберпространство формируется посредством совокупности мобильных и компьютерных устройств, при помощи которых пользователи осуществляют коммуникации между собой на расстоянии[1]. Другие определяют его как многоаспектное философское, политическое, уголовно-правовое, криминалистическое явление, которое нельзя рассматривать в усечённом формате[2].

Таким образом, можно констатировать, что киберпространство с уголовно-правовой точки зрения обладает следующими свойствами[3]:

– «киберпространство» так же, как ноосфера или биосфера, имеет свои уровни погружённости: так, существуют зоны общего доступа – ИТС «Интернет», которой может воспользоваться каждый субъект общественных отношений при наличии базовых технических устройств.

[1] Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 262.

[2] Ефремова И.А., Смушкин А.Б., Донченко А.Г., Матушкин П.А. Киберпространство как новая среда преступности // Вестн. Том. гос. ун-та. 2021. № 472. С. 249.

[3] Лихачев Н.А. Нематериальное пространство как новая форма места совершения преступления: доктринальный аспект // Юридические исследования. 2024. № 4. С. 4.

При этом активно функционируют ограниченные сети киберпространства – военные, правоохранительные, специального назначения, а также глубинный «Интернет» или Даркнет, который аккумулирует большинство преступлений в сфере информационной безопасности (незаконный оборот наркотиков, порнографии, иных запрещенных к гражданскому обороту средств, информации, полученной противоправным путем, незаконные финансовые операции и т.д.);

– как место преступления или криминогенная среда «киберпространство» косвенным образом схоже с материальной действительностью. Так же, как и в реальном мире, в нем посредством гиперссылок возможно перемещение от одного сайта к другому, получение удаленного доступа к персональным компьютерным и мобильным устройствам и т.д. При этом для пользователя пределы киберпространства остаются неограниченными и познаются аналогично окружающему его материальному миру;

– «киберпространство», равно и как объекты материальной действительности, представляет собой определенную территориальную систему с привязанностью к определенному месту, адресу, точке доступа. Так, информация хранится на определенном сервере, носителе, компьютерном устройстве, облачном хранилище, которое также имеет конечный сервер. Таким образом, в результате объекты нематериального мира, на которые посягает преступник или с помощью которых совершается преступление, имеют конечную осязаемую реальную природу и место действия;

– «киберпространство» имеет экстерриториальный или надтерриториальный характер, так как доступ к той или иной информации, распространение ее и/или вредоносного программного обеспечения, или иных предметов, запрещенных к свободному гражданскому обороту, посредством ИТС «Интернет», можно фактически совершить с территории одного государства в отношении субъекта, находящегося в пределах юрисдикции другого государства, и эти обстоятельства крайне затруднительно установить;

– «киберпространство» является частью еще более широкой социально-правовой категории – информационное пространство. Под ним понимается совокупность всех общественных отношений, связанных с хранением, обработкой, передачей, распространением, обменом, созданием информации, сведений, данных в электронной, компьютерной, телевизионной, радио, бумажной и иной форме.

Информационное пространство следует понимать как новую, не известную ранее среду психологического воздействия на общество. Подмена и умышленное искажение фактов, информационные вбросы и потоки представляют собой совокупность элементов, направленных на формирование общественного мнения, что в свою очередь может быть угрозой информационной безопасности национального характера. Так, в качестве примера можно привести антипрививочную компанию и деятельность «антиваксеров» в период пандемии COVID-19. Активное манипулирование сознанием неограниченного круга субъектов, распространение сведений недостоверного, заведомого ложного характера привело к тому, что некоторые граждане РФ избегали прививочной компании, подвергая себя и окружающих большой опасности.

Киберпространство, равно как и инфосфера, тесно связано со второй категорией представленных преступлений – деяний, связанных с распространением сведений и данных, которые могут обладать свойствами одного из обязательных признаков состава уголовно-правового деликта.

Неправомерное использования информации, манипулирование данными и их распространение становится средством и способом совершения отдельных преступлений. Реакцией законодателя стало внесение изменений в УК РФ, связанных с криминализацией ряда новых деяний:

– ст. 205^2 УК РФ «Публичные призывы к осуществлению террористической деятельности, публичное оправдание терроризма или пропаганда терроризма» – криминализация деяния произведена в 2006 г., а в 2017 г. дополнена еще одним альтернативным действием – публичной

пропагандой терроризма, которая выражается в деятельности по распространению материалов и/или информации, направленных на формировании у лица идеологии терроризма, убежденности в ее привлекательности либо представления о допустимости осуществления террористической деятельности[1];

– ст. 205^6 УК РФ «Несообщение о преступлении» – криминализация деяния произведена в 2016 г., объективная сторона выражается в бездействии и утаивании информации о совершении некоторых преступлений (террористической направленности, связанных с ядерными материалами, захватом власти или вооруженным мятежом);

– ст. 207^1 УК РФ «Публичное распространение заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан» – объективная сторона выражается в распространении заведомо ложной информации неограниченному кругу лиц об угрожающих безопасности обстоятельствах[2];

– ст. 207^2 УК РФ «Публичное распространение заведомо ложной общественно значимой информации, повлекшее тяжкие последствия» – объективная сторона соответствует преступлению, закрепленному в ст. 207^1 УК РФ, но информация обрела один отличный от предыдущей критерий – «общественно значимая»[3];

– ст. 207^3 УК РФ «Публичное распространение заведомо ложной

---

[1] О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации конвенции совета Европы о предупреждении терроризма» и Федерального закона «О противодействии терроризму»: Федеральный закон от 27 июля 2006 г. № 153-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61802/). (дата обращения: 14.01.2023 г.); О внесении изменений в Уголовный кодекс Российской Федерации в целях совершенствования мер противодействия терроризму: Федеральный закон от 29 декабря 2017 г. № 445-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_286754/. (дата обращения: 14.01.2023 г.).

[2] О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 01 апреля 2020 г. № 100-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_349082/. (дата обращения: 14.01.2023 г.).

[3] Там же.

информации об использовании Вооруженных Сил Российской Федерации, исполнении государственными органами Российской Федерации своих полномочий» – объективная сторона выражается в распространении заведомо ложной информации неограниченному кругу лиц о деятельности Вооруженных Сил РФ и органов государственной власти РФ[1];

– ст. 280 УК РФ «Публичные призывы к осуществлению экстремистской деятельности» – в 2014 г. добавлен квалифицирующий признак: «с использованием информационно-коммуникационных сетей, в том числе сети «Интернет»[2];

– ст. 280[1] УК РФ «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации» – криминализация деяния была произведена в 2013 г., объективная сторона отражает название статьи[3];

– ст. 280[3] УК РФ «Публичные действия, направленные на дискредитацию использования Вооруженных Сил Российской Федерации в целях защиты интересов Российской Федерации» – криминализация деяния произведена в 2023 г., представляет интерес в части совершения призывов, направленных на дискредитацию органов государственной власти[4];

– ст. 280[4] УК РФ «Публичные призывы к осуществлению деятельности, направленной против безопасности государства» –

[1] О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 04 марта 2022 г. № 32-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_410887/. (дата обращения: 14.01.2023 г.).

[2] О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 28 июня 2014 г. № 179-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_164858/. (дата обращения: 14.01.2023 г.).

[3] О внесении изменения в Уголовный кодекс Российской Федерации: Федеральный закон от 28 декабря 2013 г. № 433-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_156577/. (дата обращения: 14.01.2023 г.).

[4] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 18 марта 2023 г. № 58-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_442341/#dst100015/. (дата обращения: 14.01.2023 г.).

криминализация деяния осуществлена в 2022 г.[1];

– ст. 281[3] УК РФ «Организация диверсионного сообщества и участие в нем» – криминализация произведена в 2022 г., состав преступления представляет интерес в части содержания субъективной стороны – цель деяния состоит в пропаганде, оправдании либо поддержке диверсионной деятельности[2];

– ст. 282[4] УК РФ «Неоднократные пропаганда либо публичное демонстрирование нацистской атрибутики или символики…» – криминализация деяния произведена в 2022 г.[3];

– ст. 283[1] УК РФ «Незаконное получение сведений, составляющих государственную тайну» – криминализация деяния произведена в 2012 г.[4];

– ст. 284[2] УК РФ «Призывы к введению мер ограничительного характера в отношении Российской Федерации, граждан Российской Федерации или российских юридических лиц» – криминализация деяния произошла в 2022 г.[5];

– ст. 298[1] УК РФ «Клевета в отношении судьи, присяжного заседателя, прокурора, следователя, лица, производящего дознание,

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14 июля 2022 г. № 260-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_421797/. (дата обращения: 14.01.2023 г.).

[2] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 29 декабря 2022 г. № 586-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_436121/. (дата обращения: 14.01.2023 г.).

[3] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14 июля 2022 г. № 260-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_421797/. (дата обращения: 14.01.2023 г.).

[4] О внесении изменений в Уголовный кодекс Российской Федерации и в статью 151 Уголовно-процессуального кодекса Российской Федерации Федеральный закон от 12 ноября 2012 г. № 190-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_137651/. (дата обращения: 14.01.2023 г.).

[5] О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 04 марта 2022 г. № 32-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_410887/. (дата обращения: 14.01.2023 г.).

сотрудника органов принудительного исполнения Российской Федерации» – криминализация деяния осуществлена в 2012 г.[1];

– ст. 354[1] УК РФ «Реабилитация нацизма» – объективная сторона преступления характеризуется альтернативными действиями, заключающимися в распространении различной информации общественно опасного значения[2].

За последние годы было криминализировано более 14 деяний, сопряженных с распространением, сбором, хранением информации или сведений различного содержания, посягающих на информационную безопасность личности, общества и государства. В первоначальной редакции УК РФ 1996 г. было всего 17 таких деяний (ст. 128, 207, 212, 237, 275, 276, 283, 287, 297, 303, 306, 307, 310, 319, 320, 336, 354 УК РФ).

После принятия новой Доктрины 2016 г.[3] законодателем был избран путь криминализации общественно опасных деяний, совершаемых в рамках информационных отношений. Это подтверждает выдвинутый тезис об информатизации преступности – неотвратимого процесса интеграции в криминальную среду информационно-коммуникационных и кибернетических методов, технологий и специальных познаний.

В подавляющем большинстве составов ключевым обязательным или квалифицирующим признаком, относящимся к объективной стороне, является «публичность». Определение данного критерия в нормах действующего уголовного закона отсутствует, содержание неопределенно, и толкуется он

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 28 июля 2012 г. № 141-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_133284/. (дата обращения: 14.01.2023 г.).

[2] О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 05 мая 2014 г. № 128-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_162575/. (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/. (дата обращения: 14.01.2023 г.).

правоприменительными органами, исходя из конкретных обстоятельств совершенного деяния.

Законодатель поясняет критерий публичности только в содержании ст. 128^1 УК РФ – «публичное выступление» или «публичная демонстрация» и 282^4 УК РФ – «публичное демонстрирование». Публичность характеризуется определенным количеством субъектов, способных воспринимать информацию, которую распространяет лицо, совершающее преступление. По мнению ряда ученых, данный признак возникает при наличии не менее трех слушателей[1].

С одной стороны, стоит согласиться с данной позицией, так как приватный диалог предполагает наличие двух субъектов. С другой стороны, привлечение к уголовной ответственности по признаку публичности при наличии трех субъектов вызывает вопросы оценки и соотношения степени общественной опасности деяния и малозначительности преступления.

Другие противоправные деяния связаны с публичным отрицанием известных фактов и событий, попыток публичного пересмотра итогов Второй мировой и Великой Отечественной войн. Распространение подобных заведомо ложных сведений наносит ущерб общественной нравственности и фальсифицирует историю[2].

Другим важным аспектом содержания большинства составов криминализованных деяний является конкретизация объективной стороны, которая выражается в совершении призыва к осуществлению какого-либо действия (как правило террористической или экстремистской направленности).

---

[1] См.: Малинин В.В. Энциклопедия уголовного права. Т. 14. Преступления против свободы, чести и достоинства личности. СПб.: ГКА, 2010. С. 274. Шмарион В.И. Ответственность за преступления против чести и достоинства личности по российскому уголовному законодательству: дис. ... канд. юрид. наук. Ростов н/Д, 2001. С. 134.

[2] Прохоров Л.А., Бондарь Е.В. Уголовная ответственность за фальсификацию исторических сведений и искажение фактов о роли СССР в победе над германским фашизмом в Великой Отечественной войне // Гуманитарные, социально-экономические и общественные науки. 2018. № 9. С. 137.

Публичные призывы следует отличать от некоторых проявлений соучастия в преступлении. Так, ч. 4 ст. 33 УК РФ предусматривает подстрекательство, выражающееся в склонении другого лица к совершению противоправного посягательства путем уговора, подкупа. Разница заключается в направленности распространения информации:

– при подстрекательстве воздействие осуществляется на конкретное лицо, преступник желает вовлечь в противоправную деятельность определенного человека;

– публичные призывы характеризуются индивидуальной неопределенностью лиц, на которых распространяется информация, они могут быть обращены к социальной группе, населению муниципалитета, субъекта Федерации или гражданам всей страны, что кратно увеличивает общественную опасность деяния.

Важно понимать, что уголовный закон, выполняя охранительные и регулятивные функции, направлен на защиту чести, достоинства, доброго имени лица, поэтому криминализация деяний, связанных с распространением клеветнической или заведомо ложной информации, безусловно необходима.

В г. Твери районным отделом Следственного комитета РФ было возбуждено уголовное дело в связи с размещением в открытом доступе материалов, по признакам преступления, предусмотренного ст. 207[1] УК РФ. Следствием было установлено, что лицо распространило заведомо ложные сведения, согласно которым в ГБУЗ ТО «Городская клиническая больница № 7» г. Твери высокая смертность от инфекции COVID-19, в связи с чем было выделено большое количество специальных мешков для транспортировки тел умерших. В результате публикации сообщения на одной из интернет-площадок г. Твери с сообщением ознакомилось более 130 пользователей. Сведения, представленные УМВД по Тверской области, опровергают информацию, опубликованную гражданином[1].

[1] В г. Твери возбуждено уголовное дело по факту публичного распространения под видом достоверных сообщений заведомо ложной информации об обстоятельствах,

В г. Москве был вынесен приговор за совершение преступления, предусмотренного ст. 207[1] УК РФ, за распространение заведомо ложных сведений уже на более широкую аудиторию посредством публикации видеоролика под названием «Вирус любит мацу? Гибнут лучшие» в медиахостинге YouTube с аудиторией в 266000 подписчиков. Осужденный, обращаясь к неограниченному кругу пользователей, утверждал, что болезнь COVID-19 является «болезнью Фейгельсона – Якобсона», в группу риска заболеванием которой входят исключительно лица еврейской и армянской национальностей, а лица других национальностей данной инфекции не подвержены. Впоследствии он также опубликовал подобный ролик на странице в социальной сети «Вконтакте». Продолжая реализовывать свой преступный умысел, лицо выложило в медиахостинг YouTube еще один ролик, в котором утверждалось, что под видом борьбы с коронавирусной инфекцией производится массовое изъятие у здоровых людей внутренних органов и их последующая продажа для трансплантации[1].

Как показывает практика рассмотрения подобных уголовных дел, заведомо ложная информация представляет существенную угрозу информационной безопасности Российской Федерации. На примере конкретного уголовного дела видно, как лицо, выступая на многотысячную аудиторию, заявляет о биологическом/генетическом отличии представителей одних национальностей от других посредством их подверженности заболеваниям. Очевидно, что подобные заявления вызывают в обществе панические настроения, препятствуют обеспечению общественной безопасности, вакцинации, противодействию распространению эпидемий, др.

Появление подобных новых составов преступлений подтверждают

представляющих угрозу жизни и безопасности граждан // Официальный сайт Следственного комитета Российской Федерации. URL: https://tver.sledcom.ru/news/item/1455217/ (дата обращения: 10.01.2023 г.).

[1] Приговор Симоновского районного суда от 23 ноября 2020 г. № 1-285/2020 URL: https://mos-gorsud.ru/rs/nagatinskij/services/cases/criminal/details/4b008252-322c-46af-8a5a-0c2d2d4d5bc0(дата обращения: 16.06. 2023 г.).

озвученный ранее тезис о том, что информационную безопасность следует рассматривать не только со стороны обеспечения безопасности и конфиденциальности данных, но и обеспечения безопасности и законности распространения информации и недопустимости злоупотребления свободой массовой информации.

Процессы цифровизации стали благоприятной почвой для криминализации общественных отношений, а киберпространство привело к тому, что преступные деяния фактически могут быть совершены как в материальном, так и нематериальном мире. Уголовно-правовой науке предстоит оценить криминологическую роль компьютерных игр в совершении преступлений; влияние современных информационных и коммуникационных технологий на психику и преступное поведение граждан; то, как коммуникации посредством ИТС «Интернет» приводят к буллингу, сталкингу и иным формам посягательств на неприкосновенность личности, интернет-мошенничеству и т.д. Результатом подобных тенденций стало возникновение нового направления науки – цифровая криминология[1], которая посвящена осмыслению объективных процессов цифровизации общества и общественных отношений, развитию качественно новых форм и видов преступности, появлению новых криминогенных факторов.

Общественные отношения, защищаемые уголовным законом и выступающие объектом охранительного воздействия 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 объектов, запрещенных к гражданскому обороту;

[1] См.: Овчинский В. С. Криминология цифрового мира: учебник. М.: Инфра-М, 2018.

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

Объективный процесс всеобъемлющей цифровизации привел к новой социальной революции в общественных отношениях, в корне изменив порядок хранения, обмена, распространения информации во всех сферах жизнедеятельности. Это изменило и структурно-сущностные аспекты преступности, привело к криминализации ряда новых деяний, перечень которых еще 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 преступные 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 уголовно-правового и уголовно-процессуального) и правоприменительного механизмов, а также бездействия самих потерпевших.

Анализ современного уровня уголовно-правовой охраны информационных отношений позволяет сформулировать следующие уголовно-политические задачи в области обеспечения информационной безопасности:

1) модернизация уголовно-правового закона в связи с появлением качественно новых общественных отношений и их информатизацией;

2) формирование системы защиты информации, построение информационно-коммуникационной инфраструктуры.

Что касается первой задачи, следует заметить, что законодатель предпринимает попытки своевременного совершенствования соответствующих норм Особенной части УК РФ. Однако вторая задача требует более пристального внимания и системного подхода, так как современное уголовное законодательство не дает правовую оценку таким явлениям, как спаминг, фишинг, сбыт ботнета, DdoS-атаки, массовые взломы аккаунтов в социальных сетях, торговля персональными данными, в том числе в Даркнете, применение технологий блокчейна, оценка конвертируемости криптовалюты (особенно в контексте экономических преступлений, таких как дача взятки), проявления информационного экстремизма и терроризма.

Представляется, что уголовно-правовая охрана в области обеспечения

информационной безопасности в РФ должна развиваться в направлении систематизации информационного законодательства и теории информационной безопасности, выступающей объектом преступного посягательства. Разрозненность норм, содержащихся в Особенной части УК РФ и связанных с информационными отношениями, является препятствием для их развития и должного 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 программ, создаваемых в рамках технологий искусственного интеллекта. Так, «первой ласточкой» стало самоубийство в Бельгии. По данным, полученным из СМИ, житель Бельгии покончил с собой после продолжительной беседы с программой (искусственным интеллектом) чат-ботом, в результате чего у него развилась депрессия, следствием чего явился суицид[1].

Сложность данного случая в том, что это практически самообучающаяся программа, которая изначально не была сориентирована на причинение вреда здоровью или создание угрозы жизни человека. Таким образом, уголовно-правовая политика в области обеспечения информационной безопасности должна учитывать актуальные и потенциальные достижения науки и техники, адекватно реагировать на вызовы и угрозы времени.

Таким образом, подводя итог, следует сделать несколько промежуточных выводов:

– стремительное развитие информационно-коммуникационных технологий привело к формированию новых социально-правовых феноменов – киберпространства и информационного пространства. Анализируя их место в системе признаков состава преступления, характеризующих деяние, определять нематериальное пространство как место совершения преступления

[1] Бельгиец покончил с собой после шести недель общения с чат-ботом // ТАСС. 29 марта 2023. URL: https://tass.ru/proisshestviya/17399117 (дата обращения: 22.06. 2023 г.).

пока преждевременно, так как оно сводится к конкретному серверу, компьютерному устройству или компьютерным сетям;

– очевидно, что киберпространство и информационное пространство следует определять как криминальную среду со своей спецификой, контркультурой, особенностями способов и средств совершения преступлений, которая влияет на степень общественной опасности, что в некоторых случаях законодателем уже фактически отмечено (нормы Особенной части УК РФ, где совершение деяния в ИТС «Интернет» закреплено в качестве квалифицирующего признака);

– законодатель в последние 10–15 лет взял уверенный курс на криминализацию деяний, посягающих на нормальное функционирование информационных отношений, что выражается в появлении новых 14 составов преступлений, совершаемых в указанной сфере, и отсутствии тенденций к декриминализации соответствующих преступлений.

Отметим, что с данными выводами согласились подавляющее большинство опрошенных респондентов – представителей правоохранительной системы РФ: криминализацию поддержало 68% опрошенных, а подход к определению киберпространства – 73%.

2.2 Общая характеристика современной информационной преступности и отдельных ее видов

Преступления в сфере компьютерной информации в уголовно-правовой науке и практике уже стали направлением, которое определяет развитие преступности в XXI в. Со времени первичной криминализации в 1996 г. она приобрела более организованные, профессиональные и высокотехнологические черты. Цели злоумышленников также стали дифференцироваться на военные, экономические, политические, общеуголовные.

Перед анализом состояния преступности, ее характеристик необходимо

определиться с понятийно-категориальным аппаратом. Компьютерная преступность традиционно объективируется в совокупности деяний, предметом которых выступает компьютерная информация (гл. 28 УК РФ).

В настоящее время широко применяется понятие киберпреступности, которое определяется в уголовно-правовой науке по-разному. Так, некоторые ученые под киберпреступностью понимают совокупность уголовно-правовых деликтов, совершаемых в киберпространстве с помощью компьютерных систем/сетей против компьютерных систем, сетей, данных[1].

Ряд ученых трактует определения киберпреступности и интернет-преступности как понятия одной плоскости – уголовно-правовых деликтов, совершаемых на конкретной территории за установленный период времени, предметом посягательства которых выступают компьютерные устройства, компьютерные сети, программное обеспечение, носители компьютерной информации или сетевая информация.

При этом эти же самые устройства и вид информации могут выступать средством или/и способом совершения преступления[2].

Вопрос соотношения компьютерной преступности и кибепреступности в криминологической науке разрешается с нескольких позиций. Первая заключается в отождествлении этих понятий и, следовательно, преступных посягательств. Вторая разделяет их, определяя киберпреступность шире, так как относит к ней преступления, совершаемые с компьютерной информацией, в ИТС «Интернет», информационно-телекоммуникационных сетей, иных средств хранения и обработки электронной цифровой информации, которые не являются компьютерами в традиционном понимании[3].

---

[1] Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 48.

[2] Зигмунт О.А., Петровский А.В. Кибер- и интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. 2015. № 4 (34). С. 181.

[3] Липинский Д.А., Евдокимов К.Н. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2015. № 1. С. 103.

Представляется, что следует придерживаться последней позиции, в том числе потому, что киберпространство, которое как криминальная среда охватывает киберпреступления и преступления в сфере информационной безопасности, определяется гораздо шире, не ограничивается компьютерными преступлениями, традиционно сводимыми к деяниям, названным в гл. 28 УК РФ. В киберпространстве могут совершаться преступления общеуголовной направленности, предметом которых не выступает компьютерная информация. В данном случае ИТС «Интернет» выступает орудием или способом совершения противоправного посягательства. В то же время, учитывая, что для использования любого электронного устройства, в том числе для выхода в ИТС «Интернет», требуются специальные познания различного уровня, необходимо констатировать, что общественная опасность подобного рода деяний существенно выше в сравнении с аналогичными преступлениями, совершаемыми в реальном материальном и осязаемом мире.

Анализируя статистически данные ГИАЦ МВД РФ, можно сделать вывод о росте числа зарегистрированных преступлений в сфере компьютерной информации (гл. 28 УК РФ).

Таблица. Статистические показатели преступлений, совершаемых в сфере компьютерной информации (гл. 28 УК РФ)

Год (отчетный период)	Зарегистрировано	Раскрыто	Не раскрыто
2019	2883	729	2064
2020	4498	830	3250
2021	6869	1545	4734
2022	10027	1871	6972

Данные статистики показывают, что за последние 4 года преступность в сфере компьютерной информации выросла более чем в 3,5 раза, хотя показатели раскрываемости остаются на достаточно низком уровне.

Быстрый рост компьютерной преступности привел к возникновению в криминологии нового направления – цифровой криминологии в силу объективной необходимости анализа личности преступников, специфических черт преступности, ее причин и условий. Активную роль в концептуальном

осмыслении «новой преступности» сыграл В.С. Овчинский[1], отмечавший отсутствие серьезного понимания в прогнозировании развития компьютерных деликтов при их активном росте.

Анализируя социальную и структурную компоненту компьютерной преступности, он выделяет следующие категории субъектов соответствующих преступлений[2]:

– хакеры;

– хактивисты;

– преступники в сфере детской порнографии;

– «группы смерти» в ИТС «Интернет»;

– «группы травли» в ИТС «Интернет»;

– Деструктивные секты и сообщества в ИТС «Интернет»;

– различные организованные преступные сообщества в ИТС «Интернет».

Западный подход к классификации субъектов компьютерной преступности несколько отличается. Так, по данным американской IT-компании Hewlett Packard Enterprise, субъектов, осуществляющих противоправную деятельность в сфере компьютерной преступности, можно разделить на 5 категорий[3]:

– идейные хакеры-активисты (национально или государственно ориентированные хакеры) – в основе их преступной деятельности лежат идеологические и патриотические чувства или воинский долг. Как правило, имеют широкий спектр специальных технических средств, профессиональное образование и подготовку;

– хактивисты – идейно замотивированные субъекты

[1] См.: Овчинский В.С. Криминология цифрового мира: учебник. С. 64.

[2] Там же.

[3] The Business of Hacking Business innovation meets the business of hacking. Hewlett Packard Enterprise. 2016. С. 7. URL: https://static.politico.com/b9/55/4e3ce4cc41d88401e264dcacc35c/hpe-security-research-business-of-hacking-may-2016.pdf. P. 56-60. (дата обращения: 16.06. 2023 г.).

противоправной деятельности, действующие, как правило, эмоционально, их преступный умысел направлен на деструкцию и разрушение объектов информационной инфраструктуры и компьютерных сетей;

– киберпреступники – субъекты, которые профилируются на компьютерных преступлениях, как правило, они замотивированы исключительно на получение прибыли в качестве результата своей преступной деятельности;

– хакеры-эгоисты – профессиональные программисты, в основе преступной деятельности которых лежит не корыстный умысел, а желание обрести славу и признание;

– хакеры-профессионалы – занимаются противоправной хакерской деятельностью в качестве хобби или досуга, высокопрофессиональны, при совершении преступлений не преследуют корыстные цели.

Очевидно, что за годы существования и развития информационного и киберпространства в нем естественным путем сформировались собственные криминальные структуры и сообщества, имеющие свою контркультуру и уникальные черты.

Е.А. Маслакова в качестве признаков классификации субъектов компьютерной преступности предлагает выделять «особенности мотивации», «уровень профессиональной подготовки», «преступную специализацию», «психологические особенности преступника»[1].

Большинство преступников имеет молодой возраст – до 30 лет, высшее профессиональное образование в области математических наук или компьютерного программирования. При этом далеко не все лица, совершающие преступления в сфере компьютерной информации, относятся к хакерам. Особенностью преступной деятельности является практически полная анонимность, что позволяет формировать рыночную систему

[1] Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. 2014. № 1 (31). С. 120.

в глубинном Интернете, формировать организованные преступные группы и сообщества со сложной структурой и иерархией.

Организованная компьютерная преступность[1] была и остается очень узким и закрытым сообществом, которое базируется на хорошей репутации и профессионализме преступников. Репутация и доверие в сообществе является следствием демонстрации профессиональных навыков субъектов преступной деятельности. В глубинном Интернете и сетях с ограниченным доступом функционируют хакерские торговые площадки, реализующие информацию, полученную преступным путем, позволяющие организовать совершение преступления в сфере компьютерной информации (заказать кибератаку на объект).

Нередко хакерские сообщества формируются по национальному признаку и осуществляют свою деятельность, исходя из личных идеологических, политических, даже военных воззрений. Подробные действия, в том числе организованные кибератаки на критическую информационную инфраструктуру целых государств, привели к появлению в политологических, военных, юридических науках исследований, посвященных переосмыслению организованной компьютерной преступности. Их результатом стало признание новой формы вооруженного межгосударственного конфликта – кибервойны или информационной войны.

Хактивизм как социально-политическое явление представляет собой новую веху в структуре компьютерной преступности. Хактивистов все чаще определяют как представителей кибертеррористических сообществ, кибервойск «без флага», которые действуют в интересах государств[2]. Ведущие державы

---

[1] Это явление стало объектом серьезного исследовательского интереса. См., напр.: Соловьев В.С., Осипенко А.Л. Формы проявления организованной преступности в информационно-телекоммуникационной среде // Уголовная политика и культура противодействия преступности: материалы Международной научно-практической конференции памяти профессора В.Е. Квашиса (г. Краснодар, 29 сентября 2023 г.). Краснодар: Краснодарский университет МВД России, 2023. С. 263-275.

[2] Акопов Г.Л. Хактивизм – угроза информационной безопасности в информационном социуме // Государственное и муниципальное управление. Ученые записки. 2015. № 3. С. 196.

на официальном уровне стали признавать факт существования экзистенциальных угроз от кибервойск и кибертерроризма. Президент Российской Федерации В.В. Путин в 2013 г. поручил органам ФСБ РФ сформировать государственную систему предупреждения, предотвращения и ликвидации кибератак на объекты информационной инфраструктуры[1].

Одной из крупных кибертеррористических атак было внедрение компьютерного вируса Stuxnet на объекты иранской атомной электростанции в г. Бушера. Эти действия позволили вывести из строя и приостановить работу нескольких центрифуг, отвечающих за обогащение урана. Если бы вирус сумел блокировать функционирование операционной системы АЭС, то могла бы возникнуть техногенная катастрофа с выбросом радиации. Данный пример демонстрирует потенциальные возможности кибернетического воздействия на объекты критической информационной инфраструктуры, использования современных информационно-коммуникационных технологий для диверсионно-террористической и военной деятельности.

Впоследствии ряд источников, в том числе издание «Нью-Йорк Таймс» и «Лаборатория Касперского», приходили к выводам и утверждали, что подобные вредоносные программы разрабатывались службами специального назначения Израиля и США для проведения специальных операций[2].

В 2012 г. была выявлена еще одна специальная вредоносная компьютерная программа – вирус-троян Wiper, нацеленный на уничтожение баз данных, хранящихся на облачных серверах. Следствием таких кибератак явилась остановка функционирования нефтяных терминалов в Иране на несколько дней. Возникает проблема квалификации действий подобного рода: являются ли они новой разновидностью преступлений, ответственность за совершение которых должна предусматриваться нормами уголовного

[1] ФСБ поручено создать антихакерскую систему // Вести. 21 января 2013 г. URL: http://www.vesti.ru/doc.html?id=1010793 (дата обращения: 16.06. 2023 г.)

[2] Липинский Д.А., Евдокимов К.Н. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2015. № 1. С. 106.

законодательства, или же эти действия носят военный характер и должны относиться к актам агрессии.

В большинстве случаев кибератаки совершаются частными лицами, напрямую не связанными ни с органами государственной власти, ни со службами специального назначения. Вследствие этого серьёзной проблемой является квалификация ролей субъектов преступной деятельности, установление причинно-следственной связи, мотивов и главных организаторов.

Таким образом, в публичном и официально-правовом поле появляется новое определение – кибератака, в настоящий момент не имеющее законодательного закрепления. На международно-правовом уровне понимание этого явления также не сформировано. В уголовно-правовой доктрине существует несколько подходов к ее определению. Так, американский ученый, специалист в сфере международной безопасности классифицировал кибератаки как противоправные действия одного государства в отношении другого в виде проникновения в компьютерные системы или компьютерные сети с целью нанесения ущерба, выведения из строя, или уничтожения этих объектов, нарушения их естественного функционирования[1].

В отечественной практике определение кибератак с информационными войнами соотносится как частное и общее. В политологии теорией информационных войн занимались Н.П. Арапова[2], А.Б. Губарев[3], А.В. Манойло[4]. По юридической специальности защищена диссертация

[1] Clarke Richard A., Knake Robert K. Cyber war: the next threat to national security and what to do about it. OUP, 2010. P. 6.

[2] Арапова Н.П. Социально-информациологический подход в теории информационных войн: дис. ... канд. полит. наук. М., 2003. С. 2.

[3] Губарев А.Б. Информационные войны как объект политологического исследования: дис. ... канд. полит. наук. У., 2005. С. 10.

[4] Манойло А.В. «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12. Политические науки. 2019. № 2.

В.Э. Разуваева[1], в которой предложено правовое определение информационной войны как целенаправленного использования различных методов и способов в целях воздействия на социальные процессы и отношения с использованием средств информационных технологий, информационных ресурсов и коммуникаций путем создания факторов торможения, трансформации стабильности, развития, информационной, экономической и политической устойчивости государства, общества, человека в целях удержания (достижения) господства, преимущества, монополии в разных сегментах человеческого бытия[2].

Данное определение, безусловно, представляет научный интерес по причине давно наметившейся тенденции криминализации деяний, связанных с распространением информации различного характера (заведомо ложной, недостоверной, оскорбляющей и порочащей). По мнению некоторых ученых, в настоящее время Россия находится в состоянии информационной войны[3]. Действительно, усилившееся в последние десятилетие информационное давление на общество, попытки спровоцировать межнациональные, межконфессиональные конфликты открыто свидетельствуют о попытках манипуляции общественным сознанием посредством распространения различной информации.

При этом термин «информационная» война со временем трансформировался в новый подход – «когнитивную войну», которая определяется как информационное противостояние смыслов, идей, когда субъект-манипулятор умышленно распространяет в виртуальном пространстве определенную информацию, которая может быть заведомо ложной, может быть частично или полностью недостоверной.

---

[1] Разуваев В.Э. Правовые средства противостояния информационным войнам: дис. ... канд. юрид. наук. М., 2005. С. 5.

[2] Разуваев В.Э. Правовые средства противостояния информационным войнам: автореф. дис. ... канд. юрид. наук. М., 2005. С. 7.

[3] Галяшина Е., Никишин В. и др.: Фейковизация как средство информационной войны в интернет-медиа: науч.-практ. пос. М.: Блок-Принт, 2023. С. 13.

Систематическое распространение такой информации воздействует на сознание конечного потребителя, формируя у него определенные идеи, цели и идеалы – смыслы. Подобная деятельность может быть элементом объективной стороны как уже криминализованных деяний (например, ст. 212 УК РФ «Массовые беспорядки»), так и составов, которые только предстоит конструировать и имплементировать в акты действующего законодательства.

Говоря об информационном пространстве, отметим, что это особая сфера человеческой деятельности в сети, которая напрямую связана с созданием, преобразованием, распространением и потреблением информации и включает в себя как индивидуальное, так и коллективное общественное информационное сознание – все ресурсы информационного общества[1].

Информационные операции, осуществляемые в рамках описываемого выше явления, предполагают своей задачей комплексное и многоплановое воздействие на целевой объект (человека, социальную группу или общество вообще). Конечным результатом является популяризация организатора и его дальнейшее продвижение и пропаганду ценностей, идей и смыслов или же дискредитацию потерпевшего и его дальнейшее преследование, травлю и выдавливание из информационного пространства. Частью информационной войны могут быть преступления, которые, на первый взгляд, не имеют отношения к исследуемой теме, таковым является вымогательство (ст. 163 УК РФ). Следует также отметить, что уголовный закон предусматривает возможность освобождения от ответственности в случаях физического или психического принуждения к совершению преступления (ст. 39, 40 УК РФ). Однако на подавляющее большинство эпизодов действие

[1] См.: Морозов И.Л. Политический экстремизм: особенности эволюции при переходе от индустриального общества к информационному: монография. Волгоград, 2007. С. 320; Некрасова Е.В. Информационный аспект экстремизма и терроризма и деструктивные тенденции в СМИ // Вестник РУДН. Серия: Социология. 2013. № 1. С. 58.

указанных статей не распространяется. Данный пример применим в контексте шантажа, когда преступник понуждает совершить потерпевшего определенные действия для пресечения или недопущения распространения компрометирующей его лично или близких ему лиц информации. Особая общественная опасность проявляется в случаях, если эти действия связаны с распространением различной формы тайны (особенно государственной), совершением иных действий, направленных против интересов службы и государства.

Для большой части общества их публичная или профессиональная репутация является ключевым оборотным капиталам, обеспечивающим их существование и развитие, соответственно, умышленное распространение заведомо ложных или недостоверных дискредитирующих сведений представляет для них существенную потенциальную угрозу.

Отметим, что исследования информации как средства совершения преступления уже наличествуют в науке.

Так, Р.Г. Асланян понимает под информацией как средством совершения преступления в сфере экономической деятельности сведения, используемые виновным с целью посягательства на объект уголовно-правовой охраны, не обладающие какой-либо экономической, научной, исторической или иной ценностью и являющиеся ложными[1].

К отдельным элементам информационной войны следует относить преступления экстремистской и террористической направленности, совершаемые в информационном или киберпространстве, в том числе с использованием ИТС «Интернет». Конечная цель подобного рода деяний связана с продвижением радикальных идеологических учений и идей, дестабилизацией общественно-политической обстановки, оказанием влияния на ход следствия, судебных разбирательств, политические и законодательных

[1] Асланян Р.Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности: автореф. дис. ... канд. юрид. наук: Краснодар, 2016. С. 10.

процессов, выборов различного уровня. Современные технологии, в том числе возможность использования методов «Дипфейк», позволяет подделать любой голос, создать фальшивое выступление в аудио или видео формате, а уровень анонимности в ИТС «Интернет» позволяет преступнику избежать привлечения к уголовной ответственности и скрыть следы преступления. Поэтому критическое отношение к роли информационно-коммуникационных технологий в преступной деятельности представляется неправильным.

Таким образом, информацию следует рассматривать не только как предмет соответствующих преступлений, на что уже обращалось внимание ранее, но и как средство совершения преступного посягательства. Учитывая, что в последние годы активизировалась тенденция, направленная на дифференциацию противоправной информации (заведомо ложная, социально опасная, вредная и т.д.), вполне возможна криминализация новых деяний, средством совершения которых будет выступать противоправная информация.

Отдельного внимания заслуживают такие явления, как кибервойна и кибератака. Они чаще всего определяются как направления или отдельные действия в информационных войнах, связанные не с воздействием на общество путем распространения информации, а на компьютерные системы и объекты критической информационной инфраструктуры с целью их блокирования и/или уничтожения. Ключевым отличием кибератаки от иного противоправного воздействия на компьютерное устройство является направленность на подрыв, блокирование или уничтожение компьютерной сети или объекта критической информационной инфраструктуры. Иными словами, неправомерное воздействие на одно компьютерное устройство не может являться кибератакой в том случае, если она не преследует политические цели или не носит массовый характер.

Некоторые ученые придерживаются позиции, что при определении кибератаки необходимо исходить из направленности умысла и цели совершения противоправного деяния – применение силы как формы

вооруженного нападения[1]. Действительно, учитывая возможность организация кибератак на объекты критической информационной инфраструктуры, их можно квалифицировать как акт агрессии со стороны одного государства в отношении другого.

Ключевой проблемой, представляющей большую сложность при выработке унифицированного подхода к определению кибератаки, является определение видов соучастников и форм соучастия при данной деятельности, кто именно и каким образом выступает организатором, какие роли отводились соучастникам преступного посягательства – являлись ли они стихийно образовавшейся группой одиночек или членами устойчивого преступного сообщества с четким распределением ролей. Возможен и третий вариант – группа хакеров аффилирована с государством/государственной структурой или состоит на государственной службе, то есть непосредственно представляет какое-либо государство. Кибератаки совершаются различными способами – это могут быть фишинговые действия, массированные спам-атаки, попытки удаленного подключения, создание искусственной перегрузки компьютерной или информационной сети, использование уязвимостей в системе безопасности и т.д.

Так, Кировский суд г. Екатеринбурга постановил обвинительный приговор в отношении 22 членов преступного сообщества за совершение преступлений, предусмотренных ст. 159[6], 210, 272, 273 УК РФ[2]. Содеянное выразилось в использовании вируса типа «Lurk» для атаки различных, в том числе государственных, учреждений и похищении денежных средств на сумму 1,7 млрд руб.[3]

---

[1] Шинкарецкая Г.Г., Берман А.М. Кибератаки – противоправное использование цифровых технологий // Международное право. 2022. № 1. С. 43.

[2] Приговор Кировского районного суда г. Екатеринбурга. Дело № 1-1/2022 (1-1/2021; 1-3/2020; 1-52/2019; 1-650/2018). URL: http://kirovsky.svd.sudrf.ru/modules.php?name=mod search&text=&doSearch=%CD%E0%E9%F2%E8 (дата обращения: 16.06.2023 г.).

[3] Суд приговорил лидера хакерской группировки Lurk к 14 годам колонии // РБК. Общество, 14 февраля 2022 г. URL: https://amp.rbc.ru/rbcnews/society/14/02/2022/620a1ecf9a 79476a8b26419b (дата обращения: 16.06.2023 г.).

Ю.В. Грачева выделяет следующие предпосылки возникновения угроз информационной безопасности, своевременное купирование которых позволило бы минимизировать реальный ущерб от компьютерной преступности[1]:

– недостаток качественного и совершенного программного оборудования и надежного программного обеспечения;

– недостатки в работе обеспечивающих систем связи и хранения компьютерной информации;

– высокая забюрократизированность организационно-технических и государственных управленческих процессов;

– недостатки гарантийного и технического обслуживания;

Данный перечень проблем следует дополнить:

– недостаточным уровнем развития отечественного софта и программного обеспечения, его неспособности конкурировать с мировыми брендами (вследствие чего крайне затруднительно выстроить систему обеспечения информационной безопасности от преступлений, предусмотренных гл. 28 УК РФ);

– несовершенством уровня уголовного закона, требующего доработки и уточнения;

– проблемами международного взаимодействия при расследовании преступлений против информационной безопасности.

Таким образом, можно сделать следующие выводы:

– предлагается понимать кибератаку как 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

[1] Грачева Ю.В. Риски цифровизации: виды, характеристика, уголовно-правовая оценка: монография. М.: Проспект, 2022. С. 267.

воздействия на принятие ими решений, а также угроза совершения указанных действий в целях воздействия на принятие решений органами власти или международными организациями;

– проблему соотношения киберпространства и информационного пространства как места совершения компьютерных преступлений можно решить путем закрепления юрисдикции государства за его национальным сегментом ИТС «Интернет», таким образом распространив суверенитет за пределы материального мира, что позволит по-новому взглянуть на место уголовного закона в пространстве;

– понятие информационной войны должно быть закреплено в теории уголовного права, так как на международном уровне оно уже получило свое официальное и нормативное определение. 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 совершения противоправного деяния. Необходима теоретическая разработка уголовно-правового противодействия информационным войнам, определения критериев их противоправности, степени общественной опасности и последствий таковых.

2.3 Совершение преступлений с использованием ИТС «Интернет» как квалифицирующий признак деяния

Развитие информационно-телекоммуникационных технологий и систем привело к криминализации общественных отношений в сфере информационной безопасности, появлению новой нематериальной реальности – киберпространства, изменению роли и места ИТС «Интернет» в социальном взаимодействии. Таким образом, сетевое пространство и коммуникации ускорили процессы жизнедеятельности, в них внедрились новые программы,

использование которых позволяет изменять голос, изображение, видеозапись, производить иные фальсификации с информацией.

Безусловно, внедрение новых технологий является благом для большинства членов общества, упрощает общение, получение новых знаний, осуществление предпринимательской и общественной деятельности. Однако в то же время они становятся инструментом противоправного поведения, орудием или способом совершения преступления.

За последнее десятилетие законодатель ввел ряд новых составов, отличительной чертой которых является наличие квалифицирующего признака – «с использованием информационно-телекоммуникационных сетей (включая ИТС «Интернет»)». Если дифференцировать процесс криминализации по нескольким направлениям, то представить его можно подобным образом – по объекту:

– 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 (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 собственности (п «г» ч. 3 ст. 158, ст. 159^3, ст. 156^9 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).

Наиболее активно криминализация соответствующих деяний и включение соответствующего квалифицирующего признака происходили в период 2017–2022 гг. За это время было введено указанных обстоятельств более чем в 25 статей УК РФ (представлены ранее). При этом ИТС «Интернет» является зачастую не столько способом совершения деяния, сколько особой криминальной средой, позволяющей злоумышленнику упростить подготовку к реализации преступного умысла, «заметание» следов преступления. Одновременно в случае распространения социально опасных или заведомо ложных сведений в информационном пространстве существенным образом возрастает общественная опасность содеянного в силу неограниченной аудитории или объекта восприятия информации.

Одним из первых составов преступлений, осложненных использованием ИТС «Интернет» в качестве способа совершения, стало деяние, предусмотренное ст. 228^1 УК РФ (в 2012 г.). Незаконное производство и последующий сбыт наркотиков в настоящее время преимущественно осуществляется посредством использования возможностей ИТС «Интернет». Так, координация действий между организаторами, пособниками и исполнителями в ходе создания лабораторий по производству наркотических средств, обеспечение их функционирования необходимыми прекурсорами, ингредиентами осуществляется либо посредством глубинного «Интернета», известного также, как «Даркнет», или анонимных каналов в «Телеграмм». Подобная деятельность позволяет скрыть данные, позволяющие персонализировать лицо (его местоположение, номер телефона, ip-адрес, присвоив данные фиктивного прокси-сервера), то есть следы, место

и способ совершения деяния. Это существенным образом усложняет процесс выявления виновных и последующего привлечения их к уголовной ответственности, определения ролей и установления преступной связи между субъектами, времени начала и окончания совершения преступления, облегчает сокрытие следов противоправной деятельности. Зачастую организаторы остаются недосягаемыми для правоохранительных органов по причине технической невозможности их установления в ИТС «Интернет». Подобные технологии позволяют организаторам не контактировать напрямую с исполнителями и пособниками, взаимодействовать исключительно дистанционно – в том числе на межгосударственном/трансграничном уровне.

Использование ИТС «Интернет» в ходе реализации преступного умысла продолжается на стадии сбыта наркотических средств, когда активно применяется контекстная и таргетированная реклама, то есть информационные технологии, направленные на продвижение продукта в публичном пространстве. Использование анонимных каналов в «Телеграмм», сайтов-зеркал позволяет лицу, реализующему «товар», оставаться не установленным в подавляющем большинстве случаев, действуя нередко из-за пределов Российской Федерации, выводя средства, добытые преступным путем, на оффшорные счета. Таким образом, на примере незаконного производства и сбыта наркотических средств повышающий общественную опасность характер использования ИТС «Интернет» очевиден, так как это позволяет:

– сформировать устойчивую систему опосредованной коммуникации всех участников преступной группы или сообщества;

– анонимно взаимодействовать между субъектами противоправной деятельности, скрывая масштабы организованной преступной сети не только от правоохранительной системы, но и от самих участников по мере необходимости;

– оперативно заменять ликвидированные правоохранительной системой звенья преступной системы, нанимая в ИТС «Интернет» новых

курьеров и производителей наркотических средств, а также иных соисполнителей;

– быстро, эффективно и анонимно реализовывать наркосодержащую продукцию в пределах нескольких субъектов одного и более государств, использовать возможность вывода и легализации средств, добытых преступным путем, в третьи государства, находясь при этом практически в любой точке планеты, что позволяет организаторам противоправной деятельности практически всегда оставаться не устанавливаемыми.

Следствием цифровизации различных сфер общественной жизни стала криминализация отношений в экономике, введение в 2012 г.[1] в УК РФ ст. 159[6], предусматривающей ответственность за мошенничество в сфере компьютерной информации. Объективная сторона характеризуется использованием электронных устройств с целью хищения имущества собственников в форме средств цифрового платежа посредством воздействия на компьютерные сети и базы данных.

Дискуссионной является формулировка хищения в контексте возможности совершения действий подобного рода в отношении нематериального объекта, так как традиционные формы хищения применимы, как правило, к осязаемым объектам.

Само деяние может характеризоваться двумя способами:

– ввод, удаление, блокирование и модификация компьютерной информации (иными словами – совершение манипуляций с цифровыми средствами);

– осуществление иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или ИТС

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации Федеральный закон от 29.11.2012 № 207-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_164858/. (дата обращения: 14.01.2023 г.).

«Интернет»[1].

Важно отметить, что диспозиция ст. 159[6] УК РФ значительно отличается от классической подхода к мошенничеству, отраженному в ст. 159 УК РФ, предполагающей совершение хищение посредством обмана или злоупотреблением доверия. В то же время, осуществляя манипуляции с компьютерной информации, невозможно обмануть или использовать доверие лица, так как субъект не осуществляет взаимодействие с жертвой. Происходит обход, блокирование или преодоление защиты специальных технических средств, то есть обманывается неодушевленный предмет материального мира, следовательно, отсутствует психологический критерий классического мошенничества.

Это приводит к возникновению дихотомии, связанной с определением мошенничества, применительно к уголовному законодательству в целом и к диспозиции ст. 159[6] УК РФ – в частности. К тому же, отличительной особенностью такого хищения является его совершение полностью в виртуальной реальности, то есть перенос имущества из одного облачного хранилища (сервера) на другое или же переоформление права на имущество аналогичным образом. Это обстоятельство актуализирует дискуссию относительно определения киберпространства как места совершения преступления.

В то же время актуальная диспозиция ст. 159[6] УК РФ не позволяет аккумулировать весь перечень противоправных деяний, которые охватываются различными формами хищения, совершаемыми с использованием информационно-коммуникационных сетей (включая сеть «Интернет)», в частности:

– фишинг-технологии, предполагающие похищение личных

[1] О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_ 164858/. (дата обращения: 14.01.2023 г.).

персональных конфиденциальных данных пользователя посредством осуществления СПАМ-рассылки – сообщений, содержащих электронные ссылки, при переходе на которые пользователь предоставляет искомые преступником данные;

– фарминг-технологии, предполагающие скрытное перенаправление пользователя на зеркальные IP-адреса, что позволяет завладеть его персональными данными (логинами, паролями, данными доступа к электронным счетам банков, фотографиям и т.д.), что на данный момент не образует состава преступления, так как лицо не копирует, не модифицирует, не блокирует и не уничтожает компьютерную информацию, а лишь исследует её.

Подобные технологии сами по себе не образуют состав мошенничества, однако при конкретных обстоятельствах соответствующие деяния могут выступать в качестве приготовления к совершению преступления.

В 2014 г. начался процесс дифференциации уголовной ответственности за преступления экстремистской направленности. Так, в редакции ч. 2 ст. 280, ч. 1 ст. 282 УК РФ были добавлены следующие формулировки после слова «информации»: «либо информационно-телекоммуникационных сетей, в том числе сети «Интернет». Часть 2 ст. 280^1 УК РФ была дополнена конструкцией «деяния, совершенные с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет»)»[1]. Впоследствии, в 2022 г., УК РФ был дополнен ст. 280^4, п. «в» ч. 2 которой предусматривает ответственность за «публичные призывы к осуществлению деятельности, направленной против безопасности государства с использованием средств массовой информации

[1] См.: О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 28 июня 2014 г. № 179-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_164858/; О внесении изменений в статью 280^1 Уголовного кодекса Российской Федерации: Федеральный закон от 21 июля 2014 г. № 274-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_165925/#dst100011. (дата обращения: 14.01.2023 г.).

либо электронных или информационно-телекоммуникационных сетей, в том числе сети «Интернет»[1].

Одной из наиболее актуальных тенденций развития преступности в информационном и киберпространстве является информационный экстремизм. Описываемое явление не является новым, однако в последние годы практика его распространения и выявления стала масштабироваться в геометрической прогрессии.

Чаще всего при определении сущности данного определения встречается формулировка, предложенная в 2007 г. Р.В. Упорниковым: «Информационный экстремизм – это деятельность, осуществляемая с использованием информационных технологий, сопряженная с формами социально-психического и опосредованного физического деструктивного влияния, результатом которой является достижение публично нелегитимных и противоправных целей»[2].

Информационный экстремизм отличается несколькими критериями:

– публичное распространение информации, побуждающей к совершению преступлений экстремистской направленности;

– публичное распространение информации, оправдывающей идеологические течения и идеи экстремистской направленности;

– публичное распространение информации, убеждающей в необходимости совершения преступлений экстремистской направленности;

– публичное распространение информации, порождающей возникновение межэтнической, межрелигиозной, межнациональной ненависти и розни, в том числе в отношении какой-либо социальной группы.

Особая опасность информационного экстремизма связана

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации Федеральный закон от 14 июля 2022 г. № 260-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_421797/. (дата обращения: 14.01.2023 г.).

[2] Упорников Р.В. Политико-правовые технологии противодействия информационному экстремизму в России: дис. … канд. юрид. наук. Ростов н/Д, 2007. С. 56.

с общедоступностью социальных сетей и ИТС «Интернет», возможностью создания сети каналов и координации деятельности экстремистских сообществ, дезинформации населения и организации стихийных митингов, массовых беспорядков, которые могут приводить к столкновениям, наступлению тяжких последствий, захвату социальных и особо охраняемых объектов. С учетом многонационального и многоконфессионального состава Российской Федерации любые провокационные экстремистские действия государством должны жестко пресекаться.

Очевидно, что государство полностью осознает уровень общественной опасности, исходящей от различных проявлений информационного экстремизма или экстремизма в информационном пространстве. Действительно, различные формы экстремисткой и террористической деятельности стали приобретать все более широкую практику в ИТС «Интернет». Отметим, что такая преступная деятельность отличается специфической сложностью. В первую очередь, это связано с несовершенством терминологической базы, а именно, как следует определять «экстремизм в информационной среде», «экстремизм в информационном пространстве», «экстремизм информационного характера» и др.

Некоторые ученые определяют его как социально-психическое деструктивное воздействие на граждан через использование информационных технологий для достижения противоправных целей[1]. Определение экстремистской деятельности было официально закреплено в Федеральном законе от 25 июля 2002 г № 114-ФЗ «О противодействии экстремистской деятельности»[2] и представлено 13-ю различными видами действий.

Так, А.Х. Валеев отмечает, что ИТС «Интернет» является удобной площадкой для экстремистской деятельности, распространения среди

[1] Карташкин В.А., Быков И.П. Права человека и информационный экстремизм // Вестник РУДН. Серия: Социология. 2021. № 3. С. 582.

[2] О противодействии экстремистской деятельности: Федеральный закон от 25 июля 2002 г. № 114-ФЗ (ред. от 14 февраля 2024 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_37867/. (дата обращения: 01.03.2024 г.).

пользователей различных экстремистских материалов, которые в дальнейшем обменивают между собой субъекты[1].

Добавим, что ИТС «Интернет» как особое криминальное виртуальное пространство является удобной площадкой для вербовочной экстремистской деятельности, координации деятельности экстремистов и террористов, осуществления иных подготовительных к совершению преступления мероприятий и действий. Киберпространство позволяет эффективнее и быстрее распространять идеологию различных религиозно-политических течений экстремистского толка, вступать в открытую дискуссию относительно общего будущего вектора действия. Благодаря информационному пространству совершенствуются методы экстремизма: то, что ранее распространялось подпольным путем в форме вполне очевидных призывов и идей, сегодня представляет совокупность многогранных технологий в сфере PR, политологии и медиа в целом. В качестве примера можно привести способ высмеивания ценностей, идей, идеалов, репутации, что позволяет минимизировать значимость или репутацию объекта воздействия, сплотив вокруг него целевую аудиторию. Более того, использование ИТС «Интернет» в качестве способа совершения преступления позволяет не ограничивать себя временем, так как распространенная информация остается доступной, пока не будет удалена или заблокирована, а следовательно, перманентно воздействовать на неограниченную аудиторию.

В ИТС «Интернет» в качестве базовой площадки по осуществлению экстремистской деятельности (в том числе вербовочной) выделим следующее:

– использование сайтов и платформ, размещающих материалы экстремистской направленности;

– социальные сети, чат-мессенджеры (в том числе в онлайн-играх), платформы для коммуникации, через которые распространяются материалы экстремистского характера;

---

[1] Валеев А.Х. Борьба с проявлением экстремизма в сети Интернет // Бизнес в законе. 2011. № 6. С. 126.

– сообщества и сайты, относящиеся к глубинному сегменту ИТС «Интернет», позволяющему в скрытной форме осуществлять взаимодействие, координацию, распространение предметов, вещей, услуг, запрещенных к гражданскому обороту, в том числе организацию их контрабанды;

– создание личных анонимных каналов, чатов, площадок, распространяющих экстремистские идеи или же латентным образом вызывающих сочувствие к экстремистским течениям и идеям (концепция «мягкой силы» в PR-технологиях).

В настоящее время в рамках экстремизма можно выделить два основных направления:

– материальные (традиционные) формы радикальной деятельности (посягательства на основы конституционного строя, изменение государственной границы Российской Федерации, нарушение прав и свобод человека и гражданина по принципу его расы, религии и иной формы принадлежности и т.д.);

– интеллектуальный (информационный) экстремизм, предполагающий совершение целого спектра действий, таких как пропаганда идей экстремистского толка и исключительности, возбуждение ненависти, оправдание идей терроризма и террористической деятельности и т.д.

В контексте криминализации отдельных деяний экстремистского и террористического характера, совершенных с использованием ИТС «Интернет», следует выделить еще один состав преступления. Речь идет о ст. 354^1 УК РФ, предусматривающей уголовную ответственность за реабилитацию нацизма. Данное деяние содержит признак объективной стороны, характеризующий публичность деяния. Часть 1 ст. 354^1 УК РФ запрещает отрицание фактов, установленных Международным военным трибуналом, созванным по окончании Великой Отечественной и Второй мировой войн, осудивших нацистских преступников и отдельные организации (СС и СД) за совершение военных преступлений против мира и человечества.

Альтернативное деяние – распространение заведомо ложных сведений о деятельности СССР в годы Великой Отечественной войны и ее ветеранах. Действительно, борьба с этим преступлением имеет важное социально-политическое и информационное значение, так как в последние годы все более ощутимы тенденции, направленные на пересмотр итогов войны, обвинение СССР в развязывании Второй Мировой войны и ее уравнивание с Третьим Рейхом. Очевидно, что после подобных информационных кампаний следующим шагом станут судебные контрибуционные иски к Российской Федерации и ее выдавливание из международных структур, в частности из Совета Безопасности ООН.

Статья 354^1 УК РФ в п. «в» ч. 2, ч. 4 содержит квалифицирующие признаки, связанные с использованием при совершении преступления ИТС «Интернет». Подобный подход представляется вполне логичным, так как использование информационно-коммуникационных технологий позволяет задействовать наиболее массовые способы распространения необходимых данных, донося противоправные идеи и смыслы. Отметим, что в случаях с привлечением к ответственности за распространение заведомо ложных сведений крайне важным является собирание доказательств, позволяющих отграничить содеянное от добросовестного заблуждения. Составы, связанные с такой формулировкой, должны с субъективной стороны характеризоваться исключительно прямым умыслом, а также, как правило, определенным мотивом или целью совершения преступления.

В противном случае возможны эксцессы, связанные со стиранием грани между распространением заведомо ложных сведений, недостоверной информации, добросовестным заблуждением.

Следующим этапом введения использования ИТС «Интернет» в качестве квалифицирующего признака преступления стало дополнение УК РФ новыми нормами, предусматривающими уголовную ответственность за доведение до самоубийства или склонение к нему. Предысторией явилось массовое распространение сведений о действии в информационном

пространстве «групп смерти» – преступных сообществ, конечная цель которых заключалась в самоубийстве несовершеннолетних. Отличительной особенностью было использование методов психологического воздействия, которые не были предусмотрены актуальной на тот момент редакцией ст. 110 УК РФ, ограничивающей круг способов воздействия на потерпевшего указанием на физическое и психическое насилие.

В 2017 г. законодатель добавил п. «д» в ч. 2 ст. 110 УК РФ[1], содержащий квалифицирующий признак, предполагающий совершение преступления с использованием средств массовой информации или ИТС «Интернет». Дополнительно УК РФ был дополнен ст. 110^1 и 110^2, в которых указан аналогичный квалифицирующий признак, – п. «д» ч. 3 и ч. 2 соответственно. В данном случае использование киберпространства позволяет создавать организованные сообщества суицидальной направленности, в том числе на территории всей страны, что существенно повышает общественную опасность преступлений, позволяет скрыть следы преступления в результате анонимного воздействия, осуществления его из-за пределов территории Российской Федерации. Отметим, что практически сразу после введения новых составов стала формироваться судебная практика.

Так, в 2018 г. Судакским городским судом Республики Крым была привлечена к уголовной ответственности подсудимая за совершение преступления, предусмотренного ч. 5 ст. 110^1 УК РФ, с использованием ИТС «Интернет». Лицо, осознавая общественно опасный характер своих действий, намеренно создав поддельную страницу в социальной сети «В контакте», вступило в переписку с несовершеннолетней с целью склонения ее к совершению суицида. В ходе общения обвиняемая систематически давала советы потерпевшей о способах и методах совершения суицида, демонстрировала фотографии суицидального характера в виде порезанных

[1] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 29 июля 2017 г. № 248-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_37867/. (дата обращения: 20.10.2023 г.).

кистей рук, размещала информацию суицидального характера, содержащую признаки жестокого обращения и унижения человеческого достоинства, иными способами и уговорами настойчиво провоцировала несовершеннолетнюю к совершению самоубийства. Следствием действий обвиняемой стали 2 неудачные попытки суицида со стороны потерпевшей[1].

Пример наглядно демонстрирует, что использование ИТС «Интернет» позволяло подсудимой беспрепятственно взаимодействовать с потерпевшей, что облегчало реализацию преступного умысла, так как и родители, и иные близкие родственники оставались в неведении относительно круга общения ребенка в сети. Применяя технические возможности социальных сетей, лицо создало поддельный аккаунт, вводя несовершеннолетнюю в заблуждение относительно истинности своих реальных намерений. Подобная ситуация наглядно иллюстрирует особую общественную опасность использования ИТС «Интернет» в качестве способа совершения преступления.

С указанием на квалифицирующий признак, предполагающий использование ИТС «Интернет», построена ст. 128[1] УК РФ. Клеветнические сведения, распространяемые в сети, как правило, носят необратимый характер – их нельзя полностью удалить, стереть или уничтожить, а опровержение, согласно классическим законам PR-технологий, распространяется куда медленнее, чем любые компрометирующие данные. К тому же современные возможности в информационно-коммуникационной сфере позволяют создавать заведомо ложные сведения, опровергнуть которые возможно только посредством проведения специальной технической экспертизы. В частности, к таким технологиям относится подделка голоса путем написания компрометирующего текста и записи его от якобы потерпевшего или наложение лица на лицо другого человека, изображенного на фотографии или видеозаписи (дипфейк – поддельный синтез).

[1] Приговор Судакского городского суда Республики Крым от 07 мая 2018 г. URL: https://sudak--krm.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=3168813&delo_id=1540006&new=0&text_number=1 (дата обращения: 17.05.2023 г.).

В 2022 г. ст. 133 УК РФ была дополнена квалифицирующим признаком, предусмотренным п. «в» ч. 2, аналогичного содержания – с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети «Интернет»[1]. Понуждение к действиям сексуального характера состоит в оказании психического воздействия на потерпевшего и является активной формой, выраженной в совершении противоправных действий. Введение данного способа совершения преступления представляется весьма обоснованным в силу ранее упомянутых особенностей ИТС «Интернет» – удобство в подготовке, совершении и сокрытии следов преступления. Отметим, что аналогичные основания и специфика учитывались законодателем при включении соответствующего квалифицирующего признака и в иные статьи УК РФ за последние несколько лет. Однако представляется, что в настоящее время анализируемый квалифицирующий признак содержат не все статьи УК РФ, которые предусматривают преступные посягательства, нередко совершаемые с применением информационно-коммуникационных технологий.

В 2023 г. сложилась интересная судебная практика относительно квалификации использования ИТС «Интернет» для подготовки к совершению преступления, координации действий соучастников. Так, суд установил, что переписка в мессенджерах (социальных сетях) относительно подготовки и дальнейшей реализации преступного умысла должны подвергаться уголовно-правовой оценке с учетом квалифицирующего признака – с использованием ИТС «Интернет». Анализируемое уголовное дело касалось преступления, предусмотренного п. «б» ч. 2 ст. 228[1] УК РФ. Подсудимые не были согласны с приговором и апеллировали к использованию социальных сетей в личных целях, а не в деятельности, связанной с реализацией умысла. Однако

[1] О внесении изменений в Уголовный кодекс Российской Федерации и статью 280 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 06.03.2022 г. № 38-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_411047/3d0cac60971a511280cbba229d9b6329c07731f7/#dst100012. (дата обращения: 12.06.2023 г.).

Верховный Суд РФ в кассационном определении указал, что посредством использования интернет-программы обмена сообщений «подсудимый получил информацию о месте нахождения наркотического средства, а после размещения его в тайники-закладки, используя интернет-программу, сообщил о месте закладок»[1]. Поэтому доводы подсудимого об ошибочности квалификации его действий по п. «б» ч. 2 ст. 228[1] УК РФ неверны. Данная практика показывает, что, по сути, любое преступление, при подготовке или совершении которого использовались ресурсы или возможности ИТС «Интернет», должно квалифицироваться с учетом этого признака. Но далеко не каждая норма Особенной части УК РФ содержит указание на него.

Вследствие изложенного видится обоснованным расценивать совершение преступления с использованием информационно-коммуникационных технологий, в том числе ИТС «Интернет», как квалифицированный вид деяния или как обстоятельство, отягчающее наказание, на основании следующих их возможностей:

– анонимное выстраивание структуры преступной группы или преступного сообщества;

– опосредованное взаимодействие с членами преступной группы или преступного сообщества, сокрытие не только от правоохранительных структур, но и от отдельных членов преступного формирования;

– оперативное взаимодействие между членами преступной группы или преступного сообщества;

– наличие возможности оперативно заменить ликвидированное правоохранительными органами звено в преступной системе;

– анонимность подавляющего большинства организаторов преступлений, совершенных с использованием ИТС «Интернет», особенно в сферах наркопреступности, терроризма, экстремизма и мошенничества.

[1] Определение суда кассационной инстанции по делу № 49-УД23-21-А4 от 20 июля 2023 г. Верховный Суд Российской Федерации. URL: https://vsrf.ru/stor_pd f.php?id=2269520 (дата обращения: 14.09.2023 г.).

3 Посягательства на безопасность компьютерной информации в Российской Федерации: уголовно-правовая характеристика (ст. 272–274[2] УК РФ)

3.1 Неправомерный доступ к компьютерной информации

Противодействие преступлениям в сфере компьютерной информации представляет собой одно из самых актуальных направлений в развитии отечественного уголовного права. Всеобъемлющий процесс цифровизации практически полностью изменил представления человека об информации, способах ее хранения, передачи и изменения. За последние годы существенно возросли риски и угрозы, связанные с нарушением конфиденциальности различных данных – частной информации физических лиц, сохранности банковской, медицинской, налоговой и иных тайн, обеспечения неприкосновенности функционирования государственной критической инфраструктуры.

Так, только представители Сбербанка в 2022 г. заявили об обнаружении колл-центра в г. Бердянск с численностью сотрудников около 300 человек, незаконно аккумулировавших персональные данные более чем 20 млн россиян. Собранная информация в дальнейшем используется в различных мошеннических схемах, незаконно реализуется на теневых онлайн-платформах, продается в рекламные агентства для формирования рекламных сетей, применяется для запугивания лиц, к которым сведения имеют непосредственное отношение, и т.д.[1]

В связи с этим возникает закономерный интерес к оценке эффективности функционирования установлений уголовного закона, отвечающих за охрану персональных данных граждан, их достаточности,

[1] Сбербанк рассказал о раскрытой сети мошеннических колл-центров в Бердянске // RG RU. URL: https://rg.ru/2022/06/03/sberbank-rasskazal-o-raskrytoj-setimoshennicheskih-koll-centrov-v-berdianske.html?Msn=& (дата обращения: 22.10.2023 г.).

реализации принципа неотвратимости наказания, совершенства конструкции уголовно-правовых норм.

Глава 28 УК РФ в настоящее время содержит 5 статей, видовым объектом которых являются общественные отношения в сфере реализации порядка и обеспечения безопасности законного поиска, получения, передачи, производства, распространения и защиты компьютерной информации.

Объект преступления, предусмотренного ст. 272 УК РФ «Неправомерный доступ к компьютерной информации», по-разному раскрывается представителями отечественной уголовно-правовой науки. Некоторые придерживаются позиции, что это общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации создателем или иными пользователями[1], другие, – что речь идет непосредственно об охраняемой законом компьютерной информации[2]. К.Н. Евдокимов является сторонником широкого подхода при определении объекта преступного посягательства, определяя его как общественные отношения, обеспечивающие законные интересы физических и юридических лиц, а равно интересы общества и государства, реализуемые по поводу владения, пользования или распоряжения компьютерной информацией[3]. А.А. Харламова определяет объект как общественные отношения, обеспечивающие безопасность и правомерное использование компьютерной информации[4]. В.Г. Степанов-Егиянц под непосредственным объектом предлагает понимать общественные

---

[1] Юрченко И.А. Преступления против информационной безопасности: учебное пособие. М.: Проспект, 2022. С. 124.

[2] Корабельников С.М. Уголовно-правовая защита информационных отношений: учеб. пос. М.: Проспект, 2022. С. 61; Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использование информационно-коммуникационных технологий: учеб. пос. М.: ИНФРА-М, 2018. С. 23.

[3] Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации (по материалам Восточно-Сибирского округа): автореф. дис. … канд. юрид. наук. Иркутск, 2006. С. 10.

[4] Харламова А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации // Вестник Уральского юридического института МВД России. 2020. № 2. С. 163.

отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу[1].

Каждое из предлагаемых определений объекта по-своему верно, тем более учитывая, что отечественная теория объекта преступления – одно из самых обширных, спорных и многогранных явлений в отечественной уголовно-правовой доктрине, о чем справедливо пишет Е.Н. Карабанова[2].

Согласно теории состава преступления, предметом преступного посягательства, закрепленного ст. 272 УК РФ, может быть признана компьютерная информация, относящаяся к персональным данным физического лица/лиц, неопределенного (не установленного) количества лиц, сведения, обладающие статусом конфиденциальной, инсайдерской информации, относящиеся к медицинской, банковской, налоговой, государственной и иной тайне. От того, к какой именно информации осуществлен неправомерный доступ, будет зависеть дальнейшая квалификация деяния.

Согласно Федеральному закону № 149-ФЗ, информация может быть свободно использована любым субъектом, а также быть обменена и распространена между субъектами в том случае, если федеральным законодательством не установлены запреты или ограничения на свободное распространение информации или не утвержден особый порядок допуска к определенной информации (сведениям)[3].

Перечень такой информации, а также порядок доступа к ней, равно как и перечень лиц, имеющих доступ к информации подобного рода, определен

---

[1] Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): дис. … д-ра юрид. наук. М., 2016. С. 145.

[2] Карабанова Е.Н. Понятие объекта преступления в современном уголовном праве // Журнал российского права. 2018. № 6 (258). С. 70.

[3] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 № 149-ФЗ (ред. от 12 декабря 2023 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/. (дата обращения: 30.01.2024 г.).

нормами закона[1].

Традиционной в современной уголовно-правовой науке считается теория, согласно которой предметом преступления может являться исключительно объект материального мира, на который преступник имеет возможность оказать непосредственное воздействие при совершении преступного деяния[2]. Данная позиция на определенном историческом этапе, безусловно, являлась доминирующей, однако с появлением в уголовно-правовой действительности виртуальной реальности, киберпространства, «дистанционной» преступности, киберпреступлений возникает необходимость переосмысления и дополнения концепции предмета преступления. В частности, об этом писали Д.А. Калмыков[3], А.Ф. Мицкевич[4].

В рамках данной научной дискуссии существует и иная точка зрения. Так, А.В. Пелевина считает ошибочным определение компьютерной информации как предмета преступного посягательства, выступая за признание вместо нее в качестве указанного признака компьютерной техники как объекта материального мира[5].

Предпочтительнее исходить из позиции нематериального предмета преступлений, указанных в гл. 28 УК РФ, так как посягательство на само

---

[1] О государственной тайне: Закон РФ от 21 июля 1993 г. № 5485-1 (ред. от 04 августа 2023 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/con s_doc_LAW_2481/; О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. № 395-1 (ред. 12 декабря 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5842/; О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ (ред. от 06 февраля 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/con s_doc_LAW_61801/. (дата обращения: 25.11.2023 г.).

[2] Наумов А.В. Российское уголовное право: Общая часть: курс лекций. М.: Издательство БЕК, 2000. С. 163.

[3] Калмыков Д.А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны: автореф. дис. … канд. юрид. наук. Казань, 2005. С. 9.

[4] Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. 2010. № 2. С. 206.

[5] Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации // Пробелы в российском законодательстве. 2015. № 4. С. 210.

компьютерное устройство может не сочетаться с воздействием на компьютерную информацию. Например, для копирования информации с персонального компьютера пользователя посредством использования вредоносного программного обеспечения не обязательно посягать на само компьютерное устройство, его целостность, работоспособность и функциональность с точки зрения материальной действительности, так как действие происходит в киберпространстве. При этом существует вредоносное программное обеспечение, которое при использовании способно фактически вывести из строя процессор или материнскую плату, что потребует их замену. В данном случае посягательство действительно осуществляется непосредственно на компьютерное устройство как на объект материального мира[1].

Каждый человек имеет право на тайну информации, тайну частной и семейной жизни, а также право на доступ к информации, законное распространение и передачу информации[2]. В настоящее время, учитывая, что состав преступления, предусмотренного ст. 272 УК РФ, является материальным, оно признается оконченным при наступлении либо одного, либо нескольких из указанных в законе общественно опасных последствий – уничтожения, блокирования, модификации или копирования компьютерной информации.

Понятие компьютерной информации отсутствовало в первоначальной редакции настоящей статьи и было добавлено путем принятия Федерального закона № 420-ФЗ. В результате оно было определено как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от

1 Лихачев Н.А. Неправомерный доступ к компьютерной информации: направления оптимизации состава // Гуманитарные, социально-экономические т общественные науки. 2023. № 4. С. 153-157.

[2] Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 № 149-ФЗ (ред. от 12 декабря 2023 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61798/. (дата обращения: 20.02.2024 г.).

средств их хранения, обработки и передачи[1]. Дискуссионный и противоречивый характер данного определения отмечался еще в первой главе настоящей работы, поэтому вновь останавливаться на его подробном анализе нет необходимости.

Куда больший интерес вызывает определение ранее указанных общественно опасных последствий, прямую трактовку которых уголовный закон не содержит. В 2013 г. Генеральной Прокуратурой РФ был издан документ – Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации[2]. До конца 2022 г. это был единственный документ, обладающий признаками нормативности, пусть и необязательного (рекомендательного) характера, но содержащий трактовку общественно опасных последствий для ст. 272 УК РФ.

15 декабря 2022 г. было издано постановление Пленума Верховного Суда РФ № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»», которое призвано оказать существенное влияние на формирование судебной и следственной практики по делам, о преступлениях, предусмотренных гл. 28 УК РФ[3].

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07 декабря 2011 № 420-ФЗ // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_122864/. (дата обращения: 25.07.2023 г.).

[2] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М.: Генеральная Прокуратура РФ, 2013. URL: https://epp.genproc.gov.ru/web/gprf/documents. (дата обращения: 12.09.2023 г.).

[3] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 № 37 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 12.09.2023 г.).

Проведя сравнительный анализ подходов к пониманию содержания указанных общественно опасных последствий в двух документах, можно заметить, что Методические рекомендации широко трактуют общественно опасные последствия, используя формулировку «уничтожение информации» – приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления. Уничтожением информации не является переименование файла, где она содержится, а также само по себе автоматическое «вытеснение» старых версий файлов последними по времени.

Исходя из смысла данной формулировки, вред или последствия выражаются в фактической/физической утрате информации как таковой, однако проблема в том, что восстанавливаемая информация не может считаться окончательно уничтоженной. В случае полного восстановления общественно опасные последствия нивелируются, если только временное отсутствие информации не повлекло за собой причинение потерпевшему ущерба.

Постановление Пленума Верховного Суда РФ несколько иначе определяет уничтожение компьютерной информации применительно к ст. 272 УК РФ – это приведение такой информации полностью или в части в непригодное для использования состояние с целью утраты возможности ее восстановления, независимо от того, имеется ли фактически такая возможность и была ли она впоследствии восстановлена.

В данном случае существенным отличием является добавление обязательного признака субъективной стороны преступления – цели – «утрата возможности восстановления информации». В обеих версиях присутствует формулировка – «вне зависимости от возможности ее восстановления».

Тем не менее, если обратиться к реальному смыслу слова «уничтожение», то отечественные толковые словари определяют его как

«прекратить существование чего-либо, истребить»[1], «ликвидировать, разрушить, прекратить состояние»[2].

Таким образом, уничтожение предполагает наличие критерия безвозвратности – невозможности восстановления уничтоженного объекта. О необходимости определения признака «безвозвратности» также пишут А.Г. Антонов, Е.А. Зорина, Д.В. Крюков[3].

Получается, что если компьютерная информация, каким-либо образом поврежденная или удаленная преступником, впоследствии восстанавливается в полном объеме, то цель преступления, а именно – утрата возможности ее восстановления – не достигнута. Информация повреждена, временно удалена, доступ к ней ограничен, она модифицирована, но окончательно не уничтожена. В таком случае целесообразнее квалифицировать деяние как повреждение информации (электронного файла) или временное искусственное ограничение доступа к ней – блокирование (например, в случаях DDoS-атаки на сервера сайтов).

Следующий вид общественно опасных последствий, определенный законодателем, это блокирование информации. Существенных расхождений в анализируемых документах формулировки этого термина не содержат. Так, под блокированием компьютерной информации понимается 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.

В случае с модификацией компьютерной информации Методические рекомендации предусматривают вариативные примеры установленных

---

[1] Ожегов С.И. Словарь русского языка: ок. 57000 слов/ под ред. Н.Ю. Шведовой. 13-е изд., испр. М.: Просвещение, 1981. С. 742.

[2] Кузнецов С.А. Современный толковый словарь русского языка. М.: Издательский дом Ридерз Дайджест, 2004. С. 870.

[3] См.: Антонов А.Г., Зорина Е.А., Крюков Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации // Вестн. Том. гос. ун-та. Право. 2022. № 44. С. 10.

законом легальных случаев модификации программ (компьютерной информации) лицами, наделенными соответствующим правовым статусом. Позиция же Пленума заключается в придании преступного характера абсолютно любым изменениям, вносимым в компьютерную информацию преступником.

Копирование компьютерной информации в целом оба источника трактуют тождественно, предполагая 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.

Безусловно, принятие постановления Пленума Верховного Суда РФ по данной категории деяний (ст. 272–274[2] УК РФ) внесет системность в судебную и следственную практику, так как была дана юридическая оценка и характеристика видам общественно опасных последствий для ст. 272 УК РФ. Тем не менее, представленные формулировки вызывают некоторые вопросы, в первую очередь, относительно малозначительности преступного деяния и оценки степени общественной опасности. Так, в случае с блокированием, модификацией и копированием компьютерной информации предполагается, что речь идет об абсолютно любых данных, содержащихся в компьютере.

Предположим, что лицо осуществляет неправомерный доступ к информации, находящейся на электронном устройстве (смартфоне) предполагаемого потерпевшего, и, ознакомившись с его фотогалереей, скачивает (копирует) себе различные файлы. Фотографии условных пейзажей, цветов, деревьев, картинки юмористического содержания и т.д. Очевидно, что общественная опасность подобных действий приближается к нулю, тем не менее, по формальным критериям данное деяние следует квалифицировать по ч. 1 ст. 272 УК РФ. Другое дело, если бы речь шла о копировании персональных данных, например фотографии паспортных данных, интимного содержания или иных сведений, относящихся к личной, семейной тайне.

Таким образом, формально имеет место наличие признаков данного состава в деяниях, в действительности не обладающих должным уровнем общественной опасности, что ведет к необоснованному уголовного преследованию, нерациональному использованию сил и средств ОВД, что не согласуется с реальной криминальной обстановкой, так как подавляющее большинство преступлений, квалифицируемых по ст. 272 УК РФ, остаётся латентным (взломы аккаунтов в социальных сетях, получения доступа к перепискам в мессенджерах и т.д.).

Еще одной особенностью квалификации содеянного по ст. 272 УК РФ является то, что это преступление нередко совершается с целью сокрытия другого деяния или образует совокупность с другими посягательствами, предусмотренными Особенной частью УК РФ. Так, например, Ленинским районным судом г. Краснодара лицо было осуждено по ч. 2 ст. 327 УК РФ, ч. 3 ст. 272 УК РФ, ч. 2 ст. 138 УК РФ за подделку официального документа, в ходе чего был совершён неправомерный доступ к компьютерной информации с использованием служебного положения, а также нарушена тайна телефонных переговоров с использованием служебного положения[1].

При этом совокупность может также быть и с преступлениями, указанными в нормах гл. 28 УК РФ. Так, приговором Бабушкинского районного суда г. Москвы лицо было осуждено по совокупности ч. 1 ст. 272, ч. 1 ст. 273 УК РФ за использование вредоносной компьютерной программы, заведомо предназначенной для несанкционированного блокирования компьютерной информации, что привело к несанкционированному доступу к компьютерной информации сайта и ее блокированию. Обращает на себя внимание то, что, согласно приговору, подсудимый является сторонником либерального общественно-политического течения, и, хотя для вменяемых ему преступлений не предусмотрены такие квалифицирующие признаки, как

[1] Приговор Ленинского районного суда г. Краснодара от 11 мая 2017 г. по делу № 1–282/2017. URL: https://sudact.ru/regular/doc/bfZ4kLZF3mNg/ (дата обращения: 15.02.2023 г.)

совершение по политическим и экстремистским мотивам, суд специально указывает на это в приговоре[1].

Возможно, говоря о перспективе совершенствования ст. 272 УК РФ, следует подумать о введении дополнительных квалифицирующих признаков, так как совершение неправомерного доступа к компьютерной информации возможно по мотивам политической, религиозной, расовой и иных форм ненависти и вражды.

Возникают также споры относительно необходимости законодательного закрепления в УК РФ пояснения относительно сущности общественно опасных последствий. Безусловно, постановления Пленума Верховного Суда РФ играют важную роль в правовой системе РФ, применяются в гражданском, административном, арбитражном и уголовном процессах. Однако, согласно закону[2], постановления были и остаются актами толкования права, имеющими рекомендательный характер и необязательны к исполнению. Схожей позиции относительно необязательного статуса названных актов придерживается А.И. Рарог[3], М.Н. Звягинцев[4]. В противном случае может быть нарушена системность и органичность правового пространства в РФ. В любом случае, согласно ст. 1 УК РФ, уголовное законодательство РФ состоит исключительно из УК РФ и включенных в него новых федеральных законов. Использование в качестве источников уголовного законодательства иных нормативных правовых актов не допускается. При этом сущностные характеристики общественно опасных последствий, напрямую влияющих на квалификацию,

---

[1] Приговор Бабушкинского районного суда ч. 1 ст. 272 УК РФ № 01–0656/2015. URL: https://mos-gorsud.ru/rs/babushkinskij/services/cases/criminal/details/bac33fad-68c7-4d0c-87e9-ad6d61317287?respondent=%D0%A8%D0%B5%D1%81%D1%82%D0%B0%D0%BA%D0%BE%D0%B2+%D0%93.%D0%9F (дата обращения: 17.02.2023 г.).

[2] О Верховном Суде Российской Федерации: Федеральный конституционный закон от 05 февраля 2014 № 3-ФКЗ (ред. от 14 июля 2022) // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_158641/. (дата обращения: 28.10.2023 г.).

[3] Рарог А.И. Правовое значение разъяснений Пленума Верховного Суда РФ // Государство и право. 2001. № 2. С. 53.

[4] Звягинцев М.Н. О необходимости нормативного правового акта «О системе правовых актов» // Источники права: проблемы создания, систематизации и реализации: межвуз. сб. ст. / под ред. В.Я. Музюкина, В.В. Сорокина. Барнаул: АлтГУ, 2007. С. 237.

строгость и вид наказания за совершение преступления, предусмотренного ст. 272 УК РФ, содержатся в постановлении Пленума Верховного Суда РФ, что является серьезным пробелом в праве и говорит о его неопределенности.

Как показывают правоприменительная практика и научные исследования, подавляющее большинство утечек связаны с нарушением обеспечения режима конфиденциальности и тайны персональных и иных данных. Следствием этого становится их последующее распространение на возмездной основе, опубликование на различных площадках в ИТС «Интернет», направленных на торговлю информацией ограниченного доступа. Неправомерный доступ предполагает умышленное совершение действий, направленных на нарушение режима обеспечения хранения, сохранности и безопасности компьютерной информации с целью получения возможности ознакомления с ней.

Сам факт осуществления неправомерного доступа, повлекший за собой противоправное ознакомление с компьютерной информацией, подлежит криминализации, так как лицо, запомнив полученные сведения, способно их в дальнейшем воспроизвести на любом другом материальном носителе или же произвести скрытое копирование, предполагающее удаление метаданных (следов преступления), что не позволит квалифицировать деяние согласно действующей редакции уголовно-правовой нормы. В качестве примера могут служить уже упомянутые в настоящей диссертации фарминг-технологии, предполагающие скрытное перенаправление пользователя на зеркальные IP-адреса, что позволяет завладеть его персональными данными (логинами, паролями, данными доступа к электронным счетам банков, фотографиям и т.д.), что на данный момент не образует состава преступления, так как лицо не копирует, не модифицирует, не блокирует и не уничтожает компьютерную информацию, а лишь исследует её.

Видится обоснованным дополнение ст. 272 УК РФ указанием на квалифицирующий признак, связанный с совершением названного в ней деяния с передачей незаконно полученных данных через Государственную

границу РФ, а именно – перемещение компьютерной информации на материальных носителях или отправка их посредством ИТС «Интернет» на серверы, находящиеся вне юрисдикции РФ.

Учитывая вышеизложенное, предлагается изложить текст ст. 272 УК РФ в следующей редакции:

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[1].

[1] Предложенные правки в части криминализации в рамках ст. 272 УК РФ непосредственного ознакомления с информацией в ходе реализации преступного умысла на осуществление непосредственного доступа к ней поддержали 79% опрошенных респондентов, а криминализацию неправомерного доступа к компьютерной информации, сопряженного с последующей трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные, – 86%. См.: Приложение 2.

3.2 Создание, распространение и использование вредоносных компьютерных программ

Компьютерные технологии, их появление и дальнейшее развитие изменило общественные отношения и процессы жизнедеятельности до неузнаваемости. Цифровизация в последние время окончательно проникла во все сферы общества – электронный документооборот, облачные хранилища информации, «большие данные», появление первых программ с функцией самообучающегося искусственного интеллекта. Не будет преувеличением заключить, что почти у каждого пользователя его персональный смартфон или компьютер содержит данные о практически всей его жизни.

Такие электронные формы хранения информации имеют различные уязвимые моменты в операционных системах, средствах и способах защиты компьютерной информации от неправомерного вмешательства, в том числе создаваемые посредством вредоносных компьютерных программ.

Ключевой составляющей состава преступления, предусмотренного ст. 273 УК РФ, его предметом является вредоносная компьютерная программа. Законодатель, принимая УК РФ в 1996 г., внося изменения в редакцию ст. 273 УК РФ в 2011 г., не посчитал нужным дать официальное уголовно-правовое определение вредоносной компьютерной программы, определив лишь направление их использования – «несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации или нейтрализация средств защиты компьютерной информации. В науке в настоящий момент также не существует единого мнения относительно толкования данного понятия.

Обращаясь к официальным документам и актам, обладающим признаками нормативности, выделим в первую очередь «Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий», согласно которому вредоносная программа определяется как созданная или

существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы информационной (компьютерной) системы[1].

В отечественном законодательстве был принят и до сих пор действует ГОСТ от 01 февраля 2008 г. Р 50922–2006 «Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения». Согласно его п. 2.6.5 вредоносная программа предназначена для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы[2].

Обращаясь к иным подзаконным нормативным правовым актам, следует выделить постановление Правительства РФ от 31 декабря 2021 г. № 2607 «Об утверждении правил оказания телематических услуг связи». Согласно п. 2 указанных правил под вредоносным программным обеспечением понимается целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя программное обеспечение, используемое в том числе в сборе, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя, либо способное привести к ухудшению параметров функционирования абонентского терминала или сети связи[3].

Как можно судить из приведенной формулировки, позиция Правительства РФ заключается в более широком толковании понимания

---

[1] Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий: ратифицировано Федеральным законом от 01 июля 2021 № 237-ФЗ // СПС «КонсультантПлюс». http://www.consultant.ru/document/cons_doc_LAW_388782/. (дата обращения: 14.01.2023 г.).

[2] Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения: ГОСТ от 01 февраля 2008 г. Р 50922–2006 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=25219#H6bMXrTwfRTQ5b4E2. (дата обращения: 14.01.2023 г.).

[3] Об утверждении правил оказания телематических услуг связи: постановление Правительства Российской Федерации от 31 декабря 2021 г. № 2607 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_406278/. (дата обращения: 14.01.2023 г.).

и сущности вредоносных компьютерных программ, в отличие от иных нормативно-правовых актов и документов толкования.

Позиция судебных органов отражена в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37, согласно которому создание вредоносных компьютерных программ или иной вредоносной компьютерной информации представляет собой деятельность, направленную на разработку, подготовку программ (в том числе путем внесения изменений в существующие программы) или иной компьютерной информации, предназначенных для несанкционированного доступа, то есть совершаемого без согласия обладателя информации лицом, не наделенным необходимыми для такого доступа полномочиями, либо в нарушение установленного нормативными правовыми актами порядка уничтожения, блокирования, модифицирования, копирования различной компьютерной информации или нейтрализации средств ее защиты[1]. Анализируя этот акт судебного толкования, можно заключить, что подход к пониманию сущности и направленности вредоносной компьютерной программы *уже*, чем в постановлении Правительства РФ № 2607, поскольку не учитывает возможность ухудшения параметров функционирования, сбора и обработки информации с компьютерного устройства пользователя.

В уголовно-правовой науке можно встретить различные версии определения вредоносной компьютерной программы.

Так, Е.А. Русскевич определяет ее как специально написанную программу, которая после получения управления имеет возможность совершать различные несанкционированные действия, причинять вред в виде

[1] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 14.01.2023 г.).

уничтожения, блокирования, модификации или копирования информации[1].

Е.А. Маслакова придерживается традиционной формально-определенной законодателем позиции, согласно которой ключевой критерий, характеризующий вредоносную программу, – это возможность несанкционированного собственником уничтожения, блокирования, модификации либо копирования компьютерной информации[2].

М.М. Малыковцев, формулируя собственное определение вредоносной компьютерной программы, отмечает ее создание на языке программирования, а также к традиционным общественно опасным последствиям в виде уничтожения, копирования, блокирования добавляет критерий искажения информации или иное нарушение установленного законным владельцем порядка работы указанных устройств. Таким образом, автор оставляет неисчерпывающим перечень возможных неправомерных действий компьютерной программы[3].

М.А. Ефремова в качестве ключевого критерия вредоносной компьютерной программы дополнительно отмечает ее скрытное от владельца или пользователя воздействие на персональное компьютерное устройство, в результате чего он не знает о наличии такой программы и соответственно – ее действиях[4].

Е.Р. Россинская и И.А. Рядовский оценивают понятие вредоносной компьютерной программы как собирательную дефиницию, говоря о необходимости вычленения объективных свойств компьютерной

---

[1] Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием инф-коммуникационных технологий: учеб. пос. М.: ИНФРА-М, 2018. С 38-39.

[2] Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. … канд. юрид. наук. Орел, 2008. С. 68.

[3] Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. … канд. юрид. наук. М., 2007. С. 10.

[4] Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М., 2015. С. 101.

программы, что позволит ее идентифицировать как вредоносную[1].

Данная позиция представляет значительный интерес, так как любая компьютерная программа являет собой логически выстроенный, математический алгоритм, который может выполнять только определённые, встроенные создателем действия. Да, безусловно, в последние годы точные науки совершили прорыв в области компьютерных технологий с появлением программ, работающих по принципу нейросетей и ИИ (искусственного интеллекта). Следовательно, появляются и новые типы вредоносного программного обеспечения, меняются способы и цели их внедрения и последующего воздействия на персональные компьютерные устройства.

Лаборатория Касперского на сегодняшний день выделяет следующие типы вредоносного программного обеспечения[2]:

– рекламные вредоносные программы – целью их деятельности является демонстрация и отображение нежелательной для пользователя рекламы; они отправляют результаты поиска пользователя на специальные рекламные сайты, а также осуществляют сбор и анализ данных с устройства с целью дальнейшей продажи рекламодателям без согласия пользователя (такие как Fireball и Appearch);

– шпионские программы – они направлены на контроль активности, хищение конфиденциальных сведений, внедряются умышленно через уязвимости или легальные программы (перехватчики паролей, мобильное шпионское ПО, программы-сборщики Cookie-файлов и т.д.);

– программы-вымогатели – направлены на блокировку и недопущение пользователя к системе и собственным данным до момента выплаты условного выкупа за допуск. Особенно распространены в сферах,

[1] Россинская Е.Р., Рядовский И.А. Концепция вредоносных программ как способов совершения компьютерных преступлений: классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. № 5. С. 700.

[2] Какие существуют типы вредоносных программ? // Лаборатория Касперского: официальный сайт. URL: https://www.kaspersky.ru/resource-center/threats/types-of-malware (дата обращения: 20.02.2023 г.).

где почти все данные хранятся преимущественно в цифровом формате, и пользователь не имеет возможности на альтернативный доступ к собственной информации (например, CryptoLocker, Phobos);

– троянские программы – функционируют по принципу маскировки под легальные программы, доступные всем пользователям, для запуска их на персональном устройстве, что приводит к заражению, после этого злоумышленник получает возможность удаленного доступа к персональному устройству пользователя, удалению, изменению, копированию компьютерной информации и слежки за ним, нарушению работы компьютера и подключенных компьютерных сетей (например, Qbot, TrickBot)**;**

– черви – самокопирующееся вредоносное программное обеспечение, основанное на принципе поиска уязвимости в операционной системе. Используются для повреждений функционирования системы, удаления, хищения, блокирования информации;

– вирус – фрагмент компьютерного кода, встраиваемый в программное обеспечение, начинающий свое функционирование непосредственно при запуске программы. Используется для инициирования Ddos-атак, как программа-вымогатель, способен удалённо вносить изменения в персональный компьютер пользователя.

Данный перечень вредоносного программного обеспечения не является исчерпывающим, в него можно включить программы-гибриды с различными функциями, ботнет-программы (слежение за пользователем). Важным критерием при определении вредоносной компьютерной программы является ее заведомая направленность на противоправные, с уголовно-правовой точки зрения, действия, так как некоторые компьютерные программы аналогично создаются, например, для осуществления удаленного доступа или работы с информацией, но в легальных целях (дистанционной консультации программиста в случае проблемы с персональным компьютером при невозможности его транспортировки).

На официальном уровне принят и действует ГОСТ Р 57429–2017

«Судебная компьютерно-техническая экспертиза. Термины и определения», который также содержит классификацию вредоносных компьютерных программ, пусть и в усеченном в сравнении с «Лабораторией Касперского» виде[1]:

– компьютерный вирус;

– троянская программа;

– червь.

На основе анализа основных видов и направленности вредоносных компьютерных программ можно классифицировать их деятельность следующим образом:

– манипуляции с информацией, содержащейся на персональном компьютерном устройстве (уничтожение, повреждение, ознакомление, копирование, анализ и т.д.);

– осуществление слежения за персональным компьютерным устройством, в том числе за перемещением пользователя;

– получение удаленного доступа к устройству и последующее фактическое выведение персонального компьютерного устройства из строя, препятствование его непосредственного функционирования;

– использование чужого компьютерного устройства для удаленного доступа к третьему персональному устройству с целью сокрытия совершения другого преступления без ведома владельца;

– сокрытие осуществления всех неправомерных действий от непосредственного пользователя.

Состав анализируемого преступления содержит альтернативный предмет преступления – иная компьютерная информация, заведомо предназначенная для несанкционированного ее обладателем уничтожения,

[1] Судебная компьютерно-техническая экспертиза. Термины и определения: ГОСТ Р 57429–2017: утв. и введен в действие 28 марта 2017 г. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=25219#4eBizZTc1RID6We8. (дата обращения: 14.01.2023 г.).

блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации. Относительно «иной компьютерной информации» также единства мнений в научном сообществе нет. Одними авторами она определяется как базы данных, файлы с командами, которые сами по себе не являются компьютерными командами, не могут причинить вред, но при взаимодействии с ними способны проявлять свои негативные свойства[1].

Ф.Б. Гребенкин, анализируя содержание термина «иная компьютерная информация», определяет ее как любую информацию со встроенными в нее вредоносными программными кодами[2].

В иных источниках определение и сущность упомянутого понятия трактуется несколько иначе, а именно как различные инструкции или описание способов несанкционированного уничтожения, блокирования, модификации компьютерной информации[3].

А.А. Энгельгардт, определяя компьютерную информацию как предмет преступления, предусмотренного ст. 273 УК РФ, формулирует ее, исходя из ряда обязательных, по его мнению, критериев[4]:

а) это сведения, сообщения, данные;

б) представленные в форме электрических сигналов;

в) независимо от средств их хранения, обработки и передачи;

г) в виде компьютерной программы либо иной (в литературе обычно не расшифровываемой) компьютерной информации;

д) заведомо предназначенных для уничтожения, блокирования,

---

[1] Комментарий к Уголовному кодексу Российской Федерации (научно-практический) / под ред. А.И. Чучаева. М.: Проспект, 2022. С. 1223.

[2] Гребенкин Ф. Б. Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ // Вестник гуманитарного образования. 2017. № 2. С. 64.

[3] Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. 2 изд. / под ред. А.В. Бриллиантова. М.: Проспект, 2016. Т. 2. С. 592.

[4] Энгельгардт А. А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации // Право. Журнал Высшей школы экономики. 2014. №4. С. 143.

модификации, копирования компьютерной информации либо средств защиты компьютерной информации;

ж) когда на такое использование компьютерной информации отсутствует необходимая санкция.

М.А. Ефремова, комментируя определение «иная компьютерная информация», отмечает, что это не самостоятельная компьютерная программа, а электронный код, способный наносить вред устройству при взаимодействии с компьютерными программами[1].

В судебной практике привлечение лиц к уголовной ответственности за распространение или использование иной компьютерной информации встречается достаточно редко. Тем не менее, рассмотрим некоторые из них. В 2013 г. в г. Красноярске было осуждено лицо за использование и распространение иной компьютерной информации, заведомо подлежащей для нейтрализации средств защиты компьютерной информации. Примечательно, что в данном случае имелась совокупность преступлений, предусмотренных ч. 1 ст. 273 УК РФ, ч. 2 ст.146 УК РФ. Первоначально лицо нарушило авторские права, неправомерно скачав программы корпорации Майкрософт и Adobe, а впоследствии, желая реализовать эти программы посредством продажи третьим лицам, осуществило копирование иной компьютерной информации, а именно файлов – «readme.txt», содержащих серийный номер от версии программы с типом лицензии «VL», являющейся иной компьютерной информацией, позволяющей произвести установку без покупки официальной версии продукта. Для установки программного обеспечения «Adobe Photoshop CS6 Extended (Rus)» скопировал файл «ReadMe.txt», содержащий описание способа установки программы, не предусмотренного правообладателем, а также скопировал файл «adobe.photoshop.cs6.patch.exe», отключающий активацию программного

[1] См.: Ефремова М.А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ // Информационное право. 2015. № 3. С. 14.

продукта, являющийся иной компьютерной информацией»[1].

Другой иллюстрацией из судебной практики можно привести приговор Кировского районного суда г. Красноярска от 24 марта 2017 г. в отношении лица, совершившего преступление, предусмотренное ч. 2 ст. 273 УК РФ. Лицо «скопировало с сайта модифицированные файлы «kSys2.dll», «Materials.exe» и «plmisc.dll» для нейтрализации защиты программы «Аскон Компас-3D V16», которые позволяют использовать программное обеспечение без покупки официальной версии продукта, что нарушает условия установки и использования программы. Указанную компьютерную информацию вместе с программным продуктом «Аскон Компас-3D V16» 01 декабря 2016 г. подсудимый Л. Записал на имеющийся у него съемный оптический носитель. В дальнейшем, реализуя свой преступный умысел, он продал эти файлы третьему лицу[2].

Таким образом, из материалов практики видно, что иная компьютерная информация сама по себе не является вредоносной, также она не является программой, а представляет собой текстовый файл, представленный в форме электронного кода, а вот ее неправомерное использование или изменение может привести к нейтрализации средств защиты компьютерной информации, нарушению авторского права, конфиденциальности данных. Поэтому ключевым отличием вредоносной компьютерной программы от иной компьютерной информации в качестве предмета совершения преступления является критерий заведомой вредоносности программы, при этом сама программа должна быть изначально задумана и создана как вредоносная.

Объективная сторона преступления, предусмотренного ст. 273 УК РФ,

---

[1] Приговор Свердловского районного суда г. Красноярска от 2 августа 2013 г. № 1–493/2013. URL: https://sudact.ru/regular/doc/E94OlaeV9h5q/?regular-txt=&regular-case_doc=%E2%84%961-493%2F2013&regular-lawchunkinfo=&regular-date_from=&regular-date_to=&regular-workflow_stage=&regular-area=&regular-court=% =1679259851602 (дата обращения: 10.01.2023 г.).

[2] Приговор Кировского районного суда г. Красноярска от 24.03.2017 № 1–171/2017. URL: https://kirovsk--krk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=18196178&delo_id=1540006&new=0&text_number=1 (дата обращения: 10.01.2023 г.).

логично связана с предметом преступления. Она характеризуется рядом альтернативных действий, совершение хотя бы одного из которых образует состав преступления.

И.А. Юрченко следующим образом классифицирует альтернативные действия объективной стороны[1]:

– создание вредоносных программ, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты;

– распространение таких программ;

– использование подобных программ.

Данная классификация представляется неточной, так как она не охватывает действия, связанные с иной компьютерной информацией, – ее распространением и использованием в аналогичных целях. Схожим образом определяет объективную сторону Ю.В. Грачева, отмечая в ней как один из признаков деяния, связанные с иной компьютерной информацией[2]. Состав преступления является формальным и не зависит от наступления общественно опасных последствий, признается оконченным с момента совершения одного из альтернативных действий.

Создание вредоносной компьютерной программы представляется продолжительным процессом и является оконченным с момента фактической готовности программы к ее непосредственному использованию. Действия же по созданию программы можно охарактеризовать как подготовку и написание программы на языке программирования для дальнейшего использования на электронном устройстве, способном к восприятию и обработке компьютерной информации. При этом речь не идет о любой

[1] Юрченко И.А. Преступления против информационной безопасности: учебное пособие. М.: Проспект, 2022. С. 126.

[2] Грачева Ю.В. Риски цифровизации: виды, характеристика, уголовно-правовая оценка. М.: Проспект, 2022. С. 221.

компьютерной программе, а только о той, при помощи которой возможно осуществить противоправный доступ к компьютерным устройствам, сетям, системам, серверам и объектам критической информационной инфраструктуры[1].

Под использованием понимается совершение действий, направленных на применение основных функциональных особенностей программы, направленной на совершение неправомерных действий с компьютерной информацией и нейтрализацией средств защиты компьютерной информации.

Под распространением вредоносных компьютерных программ понимается их умышленная передача, продажа, предоставление в пользование, дарение неограниченному кругу лиц.

Субъективная сторона преступления характеризуется прямым умыслом. Субъект преступления – общий: вменяемое физическое лицо, достигшее 16-летнего возраста.

Анализируя перспективы развития данной уголовно-правовой нормы, стоит солидаризироваться с мнением ученых, отмечающих необходимость изменения юридической конструкции ч. 1 ст. 273 УК РФ, указывающей на альтернативные действия, связанные с вредоносными компьютерными программами, употребленными во множественном числе. В частности, об этом пишет К.Н. Евдокимов[2]. Действительно, следуя формально-юридической логике, правоприменитель не имеет возможности осуществлять привлечение к уголовной ответственности какое-либо альтернативное действие с одной программой. Подобная формулировка представляет собой серьёзную логическую ошибку, требующую коррекции.

Еще одним существенным упущением является отсутствие уголовной

---

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

[2] См.: Евдокимов К.Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. 2016. № 2 (24). С. 64.

ответственности за покупку, приобретение или получение вредоносных компьютерных программ. Общественная опасность вредоносной компьютерной программы, заведомо предназначенной для совершения неправомерных действий, на сегодняшний день очевидна. Поэтому следует предполагать, что лицо, осуществляющее приобретение подобной программы, готовится к совершению преступления, предусмотренного ст. 273 УК РФ, так как другого прямого назначения у указанных программ нет.

Учитывая, что УК РФ является по сути единственным источником уголовного права, что прямо следует из содержания ст. 1 УК РФ, следует законодательно закрепить понятие вредоносной компьютерной программы в целях совершенствования процесса квалификации и расследования преступления. Проанализировав различные подходы к понятию вредоносной компьютерной программы, можно предложить авторское её понимание – это программа, созданная на языке программирования и заведомо предназначенная для неправомерного доступа к компьютерным устройствам и ресурсам сети 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 ИТС «Интернет», нейтрализации средств защиты компьютерной информации.

Таким образом, предлагаются следующие изменения в действующую редакцию ст. 273 УК РФ:

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…

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

Вопрос о целесообразности установления уголовной ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в современной уголовно-правовой науке является дискуссионным. Связано это, в первую очередь, с тем, что данная статья применяется в судебной и следственной практике крайне редко.

Так, по данным ГИАЦ МВД РФ, в период с 2017 по 2021 г. было возбуждено всего лишь 11 дел по данной статье, причем за 2020/2021 гг. не было возбуждено ни одного уголовного дела[1]. Некоторые практики также отмечают крайне низкий уровень выявления нарушений правил эксплуатации средств хранения – 0,3% от общего числа зарегистрированных преступлений в сфере обращения охраняемой законом информации с 2010 по 2019 гг.[2]

Эти статистические показатели наглядно демонстрируют кризис применения указанной уголовно-правовой нормы, которая фактически не используется, а в случае возбуждения уголовного дела органы предварительного расследования сталкиваются с рядом процессуальных, доказательственных и криминалистических сложностей. Данная проблема на сегодняшний день свойственна всем преступлениям, предусмотренным нормами гл. 28 УК РФ, в большинстве случаев это связано с процессом доказывания и установления лица, совершившего преступление, из-за технологии блуждающего IP.

Многие представители уголовно-правовой науки справедливо критикуют диспозицию ст. 274 УК РФ, отмечая неудачность формулировки, многообразие подходов к пониманию объекта преступления как одну из приоритетных причин ее процессуальной невостребованности[3]. Следует выделить следующие точки зрения ученых на определение непосредственного объекта преступления:

---

[1] Статистика и аналитика МВД России. URL: https://xn--b1aew.xn--p1ai/folder/101762 (дата обращения 20.02.2024 г.)

[2] Родивилин И.П. Особенности характеристики состояния и структуры преступлений в сфере обращения охраняемой законом информации в современный период в Российской Федерации // Вестник Восточно-Сибирского института МВД России. 2020. № 4 (95). С. 67.

[3] См., напр.: Евдокимов К.Н. Актуальные вопросы определения объекта преступного посягательства при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2018. № 4. С. 187-195; Ягудин А.Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: дис. ... канд. юрид. наук. Казань, 2012. С. 38.

– отношения в сфере безопасности информационно-телекоммуникационных технологий[1];

– безопасность компьютерной информации, компьютерной техники, информационно-телекоммуникационных сетей и оконечного оборудования, обеспечиваемая соблюдением правил их эксплуатации[2];

– общественные отношения, обеспечивающие компьютерную безопасность и защищенность компьютерных систем[3];

– общественные отношения, гарантирующие безопасность средств хранения, обработки или передачи компьютерной информации, а также информационно-телекоммуникационных сетей и оконечного оборудования, и общественные отношения, которые предусматривают порядок доступа к информационно-телекоммуникационным сетям[4];

– общественные отношения в сфере охраны компьютерной информации[5];

– безопасность информации и систем обработки информации с использованием ЭВМ[6].

Как видно из представленной палитры мнений, проблема определения объекта преступного посягательства, запрещенного ст. 274 УК РФ, очень актуальна. Объектом данного преступления являются все же общественные отношения в сфере обеспечения исполнения или соблюдения правил эксплуатации средств хранения, обработки или передачи компьютерной

---

[1] Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. ... д-ра юрид. наук: М., 2018. С. 356.

[2] Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук: Казань, 2017. С. 82-83.

[3] Кузнецов А.П., Гарипова Н.В. Проблемы определения непосредственного объекта в преступлениях в сфере компьютерной информации // Следователь. 2008. № 7. С. 5-7.

[4] Стяжкина С.А. Уголовно-правовые особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ) // Вестник Удмуртского университета. Серия «Экономика и право». 2021. №3. С. 490-491.

[5] Российское уголовное право. Общая часть: учебник / под ред. В.П. Коняхина и М.Л. Прохоровой. М.: КОНТРАКТ, 2014. С. 640.

[6] Уголовное право России. Части Общая и Особенная: учебник. 10-е изд., перераб. и доп. / под ред. А.И. Рарога. М.: Проспект, 2019. С. 780.

информации и информационно-телекоммуникационных сетей, в том числе ИТС «Интернет», а вот предметом – непосредственно компьютерная информация, компьютерные устройства и информационно-коммуникационные сети.

Состав преступления является материальным, ч. 1 ст. 274 УК РФ предусматривает наступление общественно опасных последствий в виде крупного ущерба (сумма, превышающая 1 млн. руб.), а ч. 2 статьи – наступление тяжких последствий или угрозу их наступления. Данный признак состава преступления долгое время подвергался критике в теории и практике в связи с тем, что он оценочен и неточен[1]. Возникали вопросы, что именно следует понимать под ними – выведение из строя компьютерных сетей, невозможность работы предприятий, блокирование информационных ресурсов и т.д.

Определенную ясность внесло постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37, согласно разъяснениям которого тяжкие последствия – это длительная приостановка или нарушение работы предприятия, учреждения или организации, получение доступа к информации, составляющей охраняемую законом тайну, предоставление к ней доступа неограниченному кругу лиц, причинение по неосторожности смерти, тяжкого вреда здоровью хотя бы одному человеку и т.п.[2]

Однако названный акт толкования не смог внести полной ясности, так как возникает несколько вопросов к формулировке:

– какой период времени следует считать длительной приостановкой работы предприятия: день, два, неделя, месяц. Теоретически эту проблему

[1] См., напр.: Маякова А.С., Шелепова С.А. Компьютерные преступления: отдельные вопросы квалификации // Проблемы экономики и юридической практики. 2017. № 6. С. 191-194.

[2] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_434573/. (дата обращения: 14.01.2023 г.).

можно было бы разрешить путем определения размера упущенной выгоды простоя предприятия, эквивалентной крупному ущербу, предусмотренному ч. 1 ст. 274 УК РФ, однако на практике подобные расчеты вреда крайне маловероятны, особенно при первичной квалификации преступного деяния;

– представляется различной степень общественной опасности последствий в виде причинения смерти по неосторожности и причинения по неосторожности тяжкого вреда здоровью. Жизнь является высшей ценностью, следовательно, подобные последствия обладают большей степенью общественной опасности, что не позволяет помещать их в один ряд с вредом здоровью, не говоря уже о причинении смерти по неосторожности двум и более лицам;

– вызывает опасение чрезмерно широкое толкование тяжких последствий, а именно использование смысловой конструкции «и тому подобное», что делает перечень разновидностей тяжких последствий неограниченным, что не способствует единообразию следственной и судебной практики.

Объективная сторона преступления представлена несколькими альтернативными деяниями, которые могут быть выражены как действиями, так и бездействием. Норма является бланкетной, так как непосредственно не содержит исчерпывающий перечень правил, несоблюдение или нарушение которых является основанием для привлечения лица к уголовной ответственности. Преступление считается оконченным с момента наступления общественно опасных последствий. Отметим, что к правилам, нарушение которых образует состав преступления, не относятся те, которые связаны с ограничением доступа к компьютерной информации. Они могут быть различными, но так или иначе они возлагают на предполагаемого субъекта обязанности строгого соблюдения указанных инструкций.

Субъект преступления – специальный, физическое лицо, достигшее 16 лет, уполномоченное на осуществление специальной деятельности:

– эксплуатацию средств хранения, обработки или передачи охраняемой

законом компьютерной информации, обеспечение ее защиты и надлежащего функционирования;

– эксплуатацию информационно-телекоммуникационных сетей и оконечного оборудования, обеспечение их защиты и надлежащего функционирования.

Бланкетность нормы также проявляется в отсутствии в уголовном законе определений «средство хранения информации»[1], «средство обработки информации»[2], «средство передачи информации»[3], «информационно-телекоммуникационная сеть»[4], «оконечное оборудование»[5], которые содержатся в различных подзаконных актах.

Как уже отмечалось, в практике подобные дела встречаются крайне редко, однако одно из них можно проанализировать, сопоставив нормативно-теоретические данные с фактическими обстоятельствами конкретного совершенного преступления.

24 октября 2019 г. Саровский городской суд Нижегородской области вынес приговор в отношении лица за совершение преступлений, предусмотренных ч. 3 ст. 272, ч. 3 ст. 272, ч. 4 ст. 272, ч. 4 ст. 272, ч. 2 ст. 35, ч. 1 ст. 274 и ч. 2 ст. 273 УК РФ. На работающее в ФГУП «РФЯЦ-ВНИИЭФ» лицо были возложены должностные и трудовые обязанности по выполнению требований порядка безопасного функционирования «РФЯЦ-ВНИИЭФ»,

---

[1] Оборудование периферийное систем обработки информации. Термины и определения: ГОСТ 25868–91 от 01 января 1993 г. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZT2TCEk9pl21. (дата обращения: 14.01.2023 г.).

[2] Системы обработки информации. Термины и определения: ГОСТ 15971–90 от 01 января 1992 г. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base =OTN&n=9605#n9PbyZT2TCEk9pl21. (дата обращения: 14.01.2023 г.).

[3] Передача данных. Термины и определения: ГОСТ 17657–79 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZT2TCEk9pl21.

[4] Информационно-коммуникационные технологии в образовании. Термины и определения: ГОСТ Р 52653–2006 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZT2TCEk9pl21. (дата обращения: 14.01.2023 г.).

[5] Передача данных. Термины и определения: ГОСТ 17657–79.

сохранения государственной и коммерческой тайны и интеллектуальной собственности «РФЯЦ-ВНИИЭФ». Тем не менее, виновный умышленно, действуя из корыстной заинтересованности, договорился с другим лицом об использовании компьютерного оборудования для осуществления действий по вычислению (майнингу) криптовалюты и ее последующему обращению в свою пользу. В дальнейшем несколькими физическими лицами путем использования компьютерных устройств, устройств охлаждения и электроэнергии была создана криптоферма. В результате этих действий был осуществлен неправомерный доступ к охраняемой законом компьютерной информации, составляющей, в том числе, и предмет государственной тайны. Виновный был осужден на 3 года лишения свободы[1].

Данный пример вскрывает сразу несколько проблем, связанных с анализируемой нормой. Во-первых, предусмотренное законом наказание в виде лишения свободы на срок до двух лет по ч. 1 и до пяти лет по ч. 2 ст. 274 УК РФ видится крайне мягким, исходя из тех общественно опасных последствий, которые могут наступить в случае совершения преступления. Во-вторых, 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. В-третьих, в рамках конкретного уголовного дела лицо, совершившее преступление, нарушило правила эксплуатации средств хранения, обработки и передачи компьютерной информации и информационно-телекоммуникационных сетей из корыстных побуждений, что привело к неправомерному доступу к сведениям, составляющим государственную тайну.

В связи с изложенным предлагается следующая коррекция действующей

[1] Приговор Саровского городского суда Нижегородской области № 1–167/2019. URL: https://sarovsky-nnov.sudrf.ru/modules.php?name=sud_delo&name_op=case&case_id=11412729&case_uid=d45ac732-0fab-45e1-b96934e877aad8dd&delo_id=1540006&case_type=0&new=0&srv_num=1 (дата обращения: 20.03.2023 г.).

редакции уголовно-правовой нормы:

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…

3.4 Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Развитие информационных технологий, средств связи, коммуникаций, ИТС «Интернет» 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. В первую очередь, это, безусловно, развитие, ускорение общественной жизни, рост ее качества, доступности медицины, электроэнергии, транспорта, скорости Интернета и т.д. С другой стороны, рост зависимости общества и государства от информационных систем, отключение которых способно на продолжительный промежуток времени парализовать процессы жизнедеятельности общества и государства.

Осложнение внешнеполитической обстановки неизменно влечет увеличение количества кибератак на объекты критической информационной инфраструктуры (далее – КИИ) России. Именно существенный рост подобных преступных по своей природе и социальной философии деяний стал причиной включения в 2017 г. кардинально нового состава преступления в гл. 28 УК РФ – неправомерное воздействие на КИИ РФ (ст. 274[1])[1].

Так, по официальным данным Федеральной службы безопасности РФ, в 2016 г. на объекты КИИ было совершено 70 млн различных атак, большинство которых осуществлялось из-за пределов территории Российской Федерации[2].

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26 июля 2017 г. № 194-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_220891/. (дата обращения: 22.03.2023 г.).

[2] См.: Российская газета. 2017. 24 янв. URL: https://rg.ru/2017/01/24/v-fsb-zaiavili-o-70-mln-kiberatakah-na-informacionnye-obekty-rf.html (дата обращения: 22.03.2023 г.).

Криминализация нового деяния повлекла необходимость определения ряда понятий и правового регулирования функционирования и классификации объектов КИИ. В итоге был принят Федеральный закон 187-ФЗ[1], согласно ст. 2 которого объекты КИИ – это информационные системы, информационно-коммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры (государственных органов и учреждений, в том числе крупных значимых частных учреждений банковской сферы, здравоохранения, науки, топливно-энергетического комплекса и т.д.).

Отметим, что это не было первой попыткой законодателя закрепить официально-правовой статус КИИ. Впервые процесс формирования КИИ в Российской Федерации был инициирован в 1992 г. принятием Закона от 23 сентября 1992 г. № 3523–1 «О правовой охране программ для электронных вычислительных машин и баз данных»[2]. Само понятие объекта КИИ было использовано впервые в 1994 г. в Федеральном законе от 21 декабря 1994 г. № 68-ФЗ «О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера», который достаточно пространно определял объект КИИ как «вмешательство в функционирование которого, приведет к потере управления экономикой Российской Федерации, субъекта Российской Федерации или административно-территориальной единицы субъекта Российской Федерации, необратимому негативному изменению (разрушению) либо существенному снижению безопасности жизнедеятельности населения»[3].

---

[1] О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ (ред. от 10 июля 2023 г.) // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_220885/. (дата обращения: 22.11.2023 г.).

[2] О правовой охране программ для электронных вычислительных машин и баз данных: Закон РФ от 23 сентября 1992 г. № 3523–1 (ред. от 02 февраля 2006 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_ LAW_1007/. (дата обращения: 22.03.2023 г.). Утратил силу.

[3] О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: Федеральный закон от 21 декабря 1994 г. № 68-ФЗ (ред. от 14.04.2023 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5295/. (дата обращения: 16.10.2023 г.).

В настоящее время дополнительно действует ГОСТ[1], также содержащий определение системы информационной инфраструктуры как системы, осуществляющей управление критическим объектом или процессом, нарушение или прерывание которого влечет наступление чрезвычайной ситуации со значительными негативными последствиями (ущербу имуществу физических/юридических лиц, окружающей среде, жизни и здоровью граждан). Дополнительно были приняты Правила, определяющие обеспечение государственного контроля за объектами КИИ, которые также имеют непосредственное отношение к ст. 274[1] УК РФ[2].

Таким образом, существенный рост угрозы объектам КИИ, обеспечивающим стабильное функционирование и жизнедеятельность общества, стал причиной появления нового состава преступления.

Стоит отметить, что представители уголовно-правовой науки по-разному оценивают практическую значимость и качество анализируемой статьи УК РФ. Так, С.Д. Бражник высказывает сомнение в действенности данной нормы, а также о различии в оценке общественной опасности деяния законодателем и правоприменителем[3].

Е.А. Русскевич пишет, что подобная практика формирования диспозиции уголовно-правовой нормы противоречит отечественной традиции криминализации и использования юридической техники при конструкции

---

[1] Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: ГОСТ Р 53114–2008 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZT2TCEk9pl21. (дата обращения: 22.03.2023 г.).

[2] Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: постановление Правительства РФ от 17 февраля 2018 г. № 162 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document /cons_doc_ LAW_291398/. (дата обращения: 22.03.2023 г.).

[3] Бражник С.Д. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК РФ): мифы, реальность, перспективы // Прогресс и преемственность в российском уголовном праве (к 95-летию УК РСФСР 1926 и 25-летию УК РФ 1996 г.): материалы Всероссийской научно-практической конференции с международным участием / отв. ред. В.П. Коняхин и М.Л. Прохорова. Краснодар: Кубанский государственный университет, 2021. С. 526-540.

уголовно-правовых норм[1].

А.В. Шульга и Р.Р. Галиакбаров оценивают норму как специальный состав преступления по отношению к традиционным действующим нормам гл. 28 УК РФ, который выделяется только по специфике закрепленного предмета посягательства[2].

Ю.В. Трунцевский определяет объект названного преступления как общественные отношения, направленные на обеспечение правил эксплуатации средств хранения, передачи или же обработки охраняемой законом компьютерной информации, находящейся на объектах КИИ[3].

Я.О. Кучина рассматривает его как общественные отношения в сфере обеспечения охраны критической информационной инфраструктуры Российской Федерации от неправомерного вмешательства[4].

Ряд ученых поддерживает в целом эту точку зрения, сходным образом определяя объект и предмет преступления, рассматривая его как специальный вид в соотношении к деяниям, указанным в ст. 272, 273, 274 УК РФ, отличающийся тем, что это деяние направлено непосредственно на объект КИИ[5].

Действительно, по сути, данная статья предусматривает три самостоятельных и альтернативных состава преступления.

---

[1] Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения. Монография. М.: ИНФРА-М, 2020. С. 237.

[2] Шульга А.В., Галиакбаров Р.Р. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК РФ) // Гуманитарные, социально-экономические и общественные науки. 2018. № 5. С. 90.

[3] Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 101.

[4] Кучина Я.О. Некоторые особенности объекта преступления в ст. 274[1] УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика: сб. ст. Междунар. науч.-практ. конф. Барнаул, 2020. С. 60-63.

[5] См., напр.: Грачева Ю.В. Риски цифровизации: виды, характеристика, уголовно-правовая оценка. М.: Проспект, 2022. С. 238; Дремлюга Р.И., Зотов С.С., Павлинская В.Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. № 2. С.134.

Часть 1 ст. 274[1] в целом дублирует диспозицию ч. 1 ст. 273 УК РФ, предусматривая ответственность за создание, распространение и/или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации. Необходимо в то же время отметить отличие, которое заключается в добавлении понятия «воздействие», которое позволяет максимально широко квалифицировать деяние. В результате можно констатировать, что ч. 1 ст. 274[1] УК РФ предусматривает уголовную ответственность за создание, распространение и/или использование вредоносного программного обеспечения, а его «вредоносность» определяется любой возможностью осуществить несанкционированный доступ к объектам КИИ. Данный подход законодателя представляется в целом логичным и закономерным. Очевидно, что уровень общественной опасности предусмотренного названной статьей преступления крайне высок, особенно если речь идет об условиях чрезвычайных ситуаций, военного времени, сложной геополитической обстановки, когда подобные потенциальные действия могут вывести из строя системы управления, спутниковой связи, координации войск, получения доступа к совершенно секретной информации и т.д.

Тем не менее, законодатель допускает такое же, как в ст. 273 УК РФ упущение, не криминализуя покупку подобной программы/получение, так как ее функционал однозначен – она может быть направлена исключительно против безопасности Российской Федерации или любого другого государства. Лицо, приобретающее подобную компьютерную программу, делает это умышленно, осознавая ее содержание и свойства, а следовательно, может ее применить и скорее всего применит по прямому назначению. Кроме того, неточным является использование словосочетания «компьютерных

программ» во множественном числе, так как с точки зрения формальной логики не может образовывать основание уголовной ответственности совершение аналогичных действий, но с одной компьютерной программой.

Часть 2 ст. 274[1] УК РФ по своему содержанию логически восходит к ст. 272 УК РФ, представляя собой неправомерный доступ к компьютерной информации, содержащейся в КИИ РФ. При этом диспозиция нормы дополняется указанием на возможность использования вредоносных компьютерных программ и иной компьютерной информации, если это повлекло причинение вреда критической информационной инфраструктуре Российской Федерации. Стоит обратить внимание, что данный состав преступления, в отличие от предусмотренного в ч. 1 ст. 274[1] УК РФ, уже материальный, предполагающий наступление реальных общественно опасных последствий в виде вреда КИИ. Однако законодатель не комментирует, что собой может представлять этот вред, не дает ответ и акт судебного толкования – постановление Пленума Верховного Суда РФ № 37 от 15 декабря 2022 г.

Конечно, используя систематическое толкование всех статей гл. 28 УК РФ, можно прийти к выводу, что речь идет об уничтожении, блокировании, модификации, копировании компьютерной информации, однако уголовное право в отличие от гражданского не предусматривает возможности применения аналогии закона. Отсутствие определения степени и критериев вреда создает логическую неопределенность и конкуренцию норм (ч. 2 и ч. 5 ст. 274[1] УК РФ) в процессе квалификации, так как не совсем понятно, как отличить вред от иных тяжких последствий (понятие тяжких последствий является условно общим для всех норм гл. 28 на основании постановления Пленума ВС РФ № 37 от 15 декабря 2022 г. (их содержание уже было рассмотрено ранее).

Конструирование материального состава в свою очередь исключает квалификацию деяния, не повлекшего наступление указанных в законе последствий, как неправомерного доступа к компьютерной информации объекта КИИ априори. Например, в ситуации, когда лицо, реализуя 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 сведения, составляющие предмет государственной тайны, или осуществляет удаленное слежение за ней.

Оценивая перспективы развития указанной нормы, предлагаю ее изложение в следующей редакции:

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…

3.5 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

Статья 274^2 введена в УК РФ Федеральным законом от 14 июля 2022 г. наряду со ст. 275^1, 282^2, 280^4. Необходимость криминализации соответствующих деяний была продиктована возросшими угрозами безопасности государства в целях «повышения эффективности системы выявления, предупреждения и пресечения преступной деятельности, осуществляемой в целях подрыва основ конституционного строя,

обороноспособности страны и безопасности государства»[1].

В изначальной редакции принятого Законопроекта данная уголовно-правовая норма представлена не была, что не позволило в полной мере ознакомиться с обоснованием необходимости криминализации конкретного деяния, раскрыть в полной мере его специфику, значимость и общественную опасность. Вместе с тем технические средства противодействия угрозам (далее – ТСПУ) играют важную роль в техническом регулировании современной связи и функционирования ИТС «Интернет» на территории Российской Федерации. Исходя из этого, проведение технико-юридического анализа построения ст. 274[2] УК РФ представляет существенный доктринальный и правоприменительный интерес.

Объектом преступления, указанного в ч. 1 данной статьи УК РФ, выступают общественные отношения в сфере исполнения и соблюдения правил (порядка) установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и иных сетей связи общего пользования.

Альтернативным объектом следует признать общественные отношения в сфере соблюдения технических условий установки средств противодействия угрозам устойчивости, безопасности и целостности или требований к сетям связи при использовании указанных средств. Технические условия и правила, указанные ст. 274[2] УК РФ, закреплены в постановлении Правительства РФ от 12 февраля 2020 г. № 126[2], а также в Федеральном законе № 126-ФЗ

[1] Пояснительная записка к проекту федерального закона «О внесении изменений в уголовный кодекс российской федерации и уголовно-процессуальный кодекс Российской Федерации» // Официальный сайт Государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/130406-8 (дата обращения: 22.02.2023 г.).

[2] Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (вместе с «Правилами установки, эксплуатации и модернизации в сети связи оператора связи

«О связи»[1], приказом Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 31 июля 2019 г. № 228[2].

Формирование системы контроля и обеспечения безопасности ИТС «Интернет» посредством подключения и использования ТСПУ продиктовано положениями Доктрины информационной безопасности РФ[3] (исходя из перечня основных информационных угроз), а также принятием Федерального закона № 90-ФЗ[4], внесшим ряд изменений в закон «О связи» в контексте формирования системы национальной ИТС «Интернет».

Таким образом, в настоящее время в Российской Федерации создается система государственного регулирования и контроля за ИТС «Интернет». Это обосновано введением технико-юридических ограничений в отношении отдельный сайтов и систем, блокируемых за распространение запрещённой законом информации, запрещение отдельных онлайн-платформ или социальных сетей. Правовые ограничения создают нормативные предпосылки для технического оснащения и обеспечения решений органов государственной

технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования»). Постановление Правительства РФ от 12 февраля 2020 г. № 126 (ред. от 28 мая 2022 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_345571/.

[1] О связи: Федеральный закон от 07 июля 2003 г. № 126-ФЗ (ред. от 14 ноября 2023 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc _LAW_43224/. (дата обращения: 22.12.2023 г.).

[2] Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам: приказ Роскомнадзора от 31 июля 2019 г. № 228 (зарегистрировано в Минюсте России 11 сентября 2019 г. № 55886) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_ 43224/. (дата обращения: 19.03.2023 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/. (дата обращения: 19.03.2023 г.).

[4] О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 01 мая 2019 г. № 90-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant .ru/ document/cons_doc_LA_323815/. (дата обращения: 19.03.2023 г.).

власти. Соответственно, за нарушение или несоблюдение принимаемых норм вводится административная и уголовная ответственность.

Внедрение в систему ТСПУ в рамках Федерального закона № 90-ФЗ обосновывалось растущей угрозой со стороны США, необходимостью применения «защитных мер для обеспечения долгосрочной и устойчивой работы ИТС «Интернет» в России, повышения надёжности работы российских интернет-ресурсов»[1]. Позиция депутатов Государственной Думы РФ и членов Совета Федерации РФ понятна и в целом соответствует логике их деятельности.

Действительно, в 2018 г. и в 2023 г. в США принимались и издавались Стратегии национальной кибербезопасности. Оба документа в качестве приоритетной угрозы указывали деятельность Российской Федерации в киберпространстве, необходимости ее сдерживания и противодействия[2]. Вследствие этого государство санкционировало установление технических средств связи, которые определяют источник передаваемого трафика, способны ограничить доступ к ресурсам с запрещенной законом информацией посредством блокирования сетевых адресов и пропуска проходящего между ними трафика.

Кроме того, был инициирован процесс создания инфраструктуры, позволяющей автономно функционировать отечественным интернет-ресурсам в случае их отключения (операторов связи) от зарубежных корневых систем ИТС «Интернет».

Обращаясь к уголовно-правовому анализу состава преступления, в первую очередь необходимо отметить его формальную конструкцию. Норма

---

[1] Пояснительная записка к проекту Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации» // Официальный сайт Государственной Думы РФ // URL: https://sozd.duma.gov.ru/bill/608767-7 (дата обращения: 19.03.2023 г.).

[2] Стратегия национальной кибербезопасности США. Сентябрь 2018 г. URL: https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_USA_2018.pdf (дата обращения: 22.02.2023 г.); National cybersecurity strategy of USA march 2023. URL: http://pentagonus.ru/doc/ National_Cybersecurity_Strategy_03_2023.pdf. P. 14-20 (дата обращения: 22.02.2023 г.).

включает административную преюдицию, то есть привлечение лица к уголовной ответственности возможно в случае совершения им в определенный период времени аналогичного административного правонарушения, предусмотренного нормами КоАП РФ, за которое оно было подвергнуто административному наказанию. Соответствующее правонарушение указано в ч. 2 ст. 13.42 КоАП РФ.

Диспозиция ст. 274^2 УК РФ является бланкетной, и фактическое содержание указанного в ней посягательства определено в различных нормах отечественного законодательства. Правовым основанием для привлечения к юридической ответственности (сначала административной, а впоследствии и уголовной) по сути является нарушение требований, предусмотренных постановлением Правительства РФ № 126 и приказом Роскомнадзора № 228.

Часть 2 ст. 274^2 УК РФ предусматривает ответственность за нарушение требований, связанных с осуществлением пропуска интернет-трафика через ТПСУ. Отметим, что данная норма аналогично ч. 1 статьи содержит указание на административную преюдицию (ст. 13.42.1 КоАП РФ[1]). Техническая правила контроля сформулированы в приказе Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации № 44 от 26 января 2022 г.[2] Дополнительным основанием для квалификации деяния по ч. 2 анализируемой статьи является нарушение положений, предусмотренных постановлением Правительства РФ № 127 от 12 февраля 2020 г[3]. Этот акт регулирует порядок управления сетью связи общего пользования, определяет

[1] Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 11 марта 2024 г.) // СПС «КонсультантПлюс». https://www.consultant.ru/document/ cons_doc_LAW_34661/ (дата обращения: 22.02.2023 г.).

[2] Об утверждении Требований к порядку пропуска трафика в сетях передачи данных: Приказ Минцифры России от 26 января 2022 г. № 44 (зарегистрировано в Минюсте России 28 февраля 2022 г. № 67538) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_410516/ (дата обращения: 22.02.2023 г.).

[3] Об утверждении Правил централизованного управления сетью связи общего пользования: Постановление Правительства РФ от 12 февраля 2020 г. № 127 (ред. от 17 декабря 2021 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_345574/ (дата обращения: 22.02.2023 г.).

виды и перечень угроз устойчивости, безопасности и целостности ИТС «Интернет».

Содержание субъективной стороны непосредственно в диспозиции уголовно-правовой нормы не отражено. Исходя из фактического содержания статьи, она характеризуется умыслом в отношении нарушения или несоблюдения указанных ранее правил. Квалификация в данном случае будет производиться на основании определения деяния в каждом конкретном случае, исходя из действия/бездействия лица, его роли в совершении преступления.

Субъект преступления – специальный: это либо должностное лицо, либо индивидуальный предприниматель, то есть вменяемое физическое лицо, достигшее возраста 18 лет. Следует отметить, что в примечании к ст. 274^2 УК РФ содержится достаточно интересное определение должностного лица – «лицо, … выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации». Таким образом, в уголовном законе возникает дихотомия, выражающаяся в наличии данного определения и понятия, содержащегося в примечании к ст. 285 УК РФ и распространяющегося на статьи гл. 30 УК РФ. Представляется не вполне корректным, что одно и то же определение в рамках одного нормативного правового акта толкуется совершенно по-разному и охватывает «противоположных» лиц (государственные служащие и работники коммерческих организаций).

Уголовно-правовая характеристика и анализ объективных и субъективных признаков рассматриваемого состава преступления осложняется отсутствием правоприменительной практики вследствие сравнительно небольшого периода времени, прошедшего с момента криминализации деяния. В силу этого обстоятельства представляется затруднительным оценивать перспективы применения и исследуемой статьи, а также выявить проблемы, которые могут возникнуть в ходе квалификации и инкриминирования соответствующего преступления.

Таким образом, подводя итог рассмотрению, осуществленному в настоящей главе, можно сделать ряд выводов:

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

– вместе с тем содержание диспозиций почти всех норм не вполне совершенно, в нем усматривается ряд неточностей и неопределенностей, которые активно критикуются представителями уголовно-правовой науки;

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

ЗАКЛЮЧЕНИЕ

Уголовно-правовое обеспечение информационной безопасности представляет одно из наиболее актуальных направлений развития уголовного законодательства Российской Федерации. Проведенное теоретико-прикладное исследование позволило оценить современное состояние уголовного закона РФ в сфере регламентации ответственности за посягательства на информационную безопасность, в первую очередь, за преступления в сфере компьютерной безопасности. В результате сформулирован ряд выводов, направленных на развитие уголовно-правовой доктрины и на совершенствование действующего законодательства в соответствующей их части:

И в отечественном законодательстве в целом, и в УК РФ, в частности, не содержится ряда ключевых понятий и определений, так или иначе связанных с реализацией ответственности за посягательства на информационную безопасность. Следует четко определить понятие информации, персональных данных, личной и семейной тайны, частной жизни лица, выделив их критерии и признаки, чтобы отграничить любую информацию от той, которая подлежит уголовно-правовой охране, поскольку 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 предмет определенных преступлений, однако требует конкретизации (термин встречается более чем в 18 кодексах российского права, но везде имеет разное значение).

В результате проведенного анализа 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 ознакомление с ними, их распространение, копирование, изменение, уничтожение, а также порядок и

форма хранения, подлежит императивному правовому регулированию, нарушение которого влечет уголовную ответственность.

Информационную безопасность в контексте теории уголовного права необходимо рассматривать с нескольких позиций:

Информационную безопасность в контексте уголовно-правовой теории 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.

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 объектов, 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 общества, представителей профессионального и научного сообщества запроса на модернизацию уголовного и уголовно-процессуального законодательства в сфере обеспечения информационной безопасности.

Объективный процесс всеобъемлющей цифровизации привел к новой социальной революции в общественных отношениях, в корне изменив порядок хранения, обмена, распространения информации во всех сферах жизнедеятельности. Это изменило и структурно-сущностные аспекты преступности, привело к криминализации ряда новых деяний, перечень, которых еще будет дополняться. Преступления, направленные 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 преступные 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 уголовно-правового и уголовно-процессуального) и правоприменительного механизмов, а также бездействия самих потерпевших.

Преступления, именуемые как «информационные», «компьютерные», «киберпреступления» и т.п., предлагается объединить в общую группу – «преступления против информационной безопасности» и определить 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 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 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).

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 место уголовного закона в пространстве.

Отметим, что подобный вывод поддержали 69% опрошенных респондентов из числа следователей МВД России, СК РФ, судей федеральных судов общей юрисдикции. При этом совершение преступления с использованием информационно-телекоммуникационных технологий в том числе сети «Интернет» следует оценивать, как обстоятельство, отягчающее деяние, из-за упрощения к приготовлению, приисканию способа и орудия совершения, последующего сокрытия следов преступления.

В процессе рассмотрения вопросов уголовно-правовой политики противодействия преступлениям против информационной безопасности разработано 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.

Указанное определение было предложено в ходе анкетирования опрошенным следователям МВД России, СК РФ, судьям федеральных судов общей юрисдикции, из которых 75% поддержали представленную дефиницию.

Анализ международно-правовых аспектов противодействия преступлениям в сфере информационной безопасности привел к выводу о настоятельной необходимости принятия 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.

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.

В диссертации обоснован комплекс предложений по изменению ряда статей Особенной части УК РФ, в частности, содержащихся в гл. 28 УК РФ («Преступления в сфере компьютерной информации»), направленных на совершенствование уголовно-правового противодействия преступлениям против информационной безопасности (представлен в приложении 1 к диссертации).

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Нормативные правовые акты

1.1 Нормативные правовые акты и иные официальные материалы Российской Федерации

1 Конституция Российской Федерации (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01 июля 2020) // СПС «КонсультантПлюс». URL: http://www.co№sulta№t.ru/docume№t/c o№s_doc_LAW_28399/.

2 О Верховном Суде Российской Федерации Федеральный конституционный закон от 05 февраля 2014 № 3-ФКЗ (ред. от 14 июля 2022) // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_158641/.

3 Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (ред. от 06 апреля 2024) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document /cons_doc_LAW_10699/.

4 Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ (ред. от 06 апреля 2024) // СПС «КонстультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_34481/.

5 Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. № 195-ФЗ (ред. от 06 апреля 2024 г.) // СПС «КонсультантПлюс». https://www.consultant.ru/document/cons_doc_LAW_34661/.

6 Гражданский кодекс Российской Федерации (ГК РФ) № 51-ФЗ (ред. от 11 марта 2024) // СПС «КонсультантПлюс». URL: https://www.consultan t.ru/document/cons_doc_ LAW_5142/.

7 Об информации, информационных технологиях и о защите

информации: Федеральный Закон от 27 июля 2006 г. № 149-ФЗ (ред. от 12 декабря 2023) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/?ysclid=lfs4b5a1bp112283080.

8 О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ. (ред. от 06 февраля 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_61801/.

9 О безопасности: Федеральный закон от 28 декабря 2010 г. № 390-ФЗ (10 июля 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_ LAW_ 108546/.

10 О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О ратификации конвенции совета Европы о предупреждении терроризма» и Федерального закона «О противодействии терроризму»: Федеральный закон от 27 июля 2006 г. № 153-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru /document/cons_doc_LAW_61802/.

11 О внесении изменений в Уголовный кодекс Российской Федерации в целях совершенствования мер противодействия терроризму: Федеральный закон от 29 декабря 2017 г. № 445-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_286754/.

12 О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 01 апреля 2020 г. № 100-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_349082/.

13 О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 04 марта 2022 г. № 32-ФЗ // СПС

«КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_410887/.

14 О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 28 июня 2014 г. № 179-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_164858/.

15 О внесении изменения в Уголовный кодекс Российской Федерации: Федеральный закон от 28 декабря 2013 г. № 433-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_156577/.

16 О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 18 марта 2023 г. № 58-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_442341/#dst100015/.

17 О связи: Федеральный закон от 07 июля 2003 г. № 126-ФЗ. (ред. от 04 августа 2023 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/d ocument/cons_doc _LAW_43224/.

18 О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации»: Федеральный закон от 01 мая 2019 г. № 90-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc _LA_323815/.

19 О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07 декабря 2011 № 420-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons _doc_LAW _122864/.

20 О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 29 декабря 2022 г. № 586-ФЗ // СПС

«КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_436121/.

21 О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14 июля 2022 г. № 260-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_421797/.

22 О внесении изменений в Уголовный кодекс Российской Федерации и в статью 151 Уголовно-процессуального кодекса Российской Федерации Федеральный закон от 12 ноября 2012 г. № 190-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_137651/.

23 О внесении изменений в Уголовный кодекс Российской Федерации и статьи 31 и 151 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 04 марта 2022 г. № 32-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_410887/.

24 О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 28 июля 2012 г. № 141-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_133284/.

25 О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 05 мая 2014 г. № 128-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_ 162575/.

26 О внесении изменений в отдельные законодательные акты Российской Федерации: Федеральный закон от 28 июня 2014 г. № 179-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_164858/.

27 О защите населения и территорий от чрезвычайных ситуаций природного и техногенного характера: Федеральный закон от 21 декабря 1994

г. № 68-ФЗ. (ред. от 14 апреля 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_5295/.

28 О внесении изменений в статью 280.1 Уголовного кодекса Российской Федерации: Федеральный закон от 21 июля 2014 г. № 274-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_165925/#dst100011.

29 О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 29 июля 2017 г. № 248-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_37867/.

30 О государственной тайне: Закон РФ от 21 июля 1993 г. № 5485–1 (ред. от 04 августа 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_ doc_LAW_2481/.

31 О банках и банковской деятельности: Федеральный закон от 2 декабря 1990 г. № 395–1 (ред. 12 декабря 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru /document/cons_doc_LAW_5842/.

32 О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ. (ред. 14 июля 2022) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/docume nt/cons_ doc_LAW_61801/.

33 О противодействии экстремистской деятельности: Федеральный закон от 25 июля 2002 г. № 114-ФЗ (ред. 14 февраля 2024) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_37867/.

34 О внесении изменений в Уголовный кодекс Российской Федерации и статью 280 Уголовно-процессуального кодекса Российской Федерации: Федеральный закон от 06 марта 2022 г. № 38-ФЗ // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_411047/3 d0cac60971a511280cbba229d9b6329c07731f7/#dst100012.

35 О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской

Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26 июля 2017 г. № 194-ФЗ // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_ LAW_220891/.

36 О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26 июля 2017 г. № 187-ФЗ. (ред. от 10 июля 2023) // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_ LAW_220885/.

37 О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07 декабря 2011 № 420-ФЗ // СПС КонсультантПлюс. URL: http://www.consultant.ru/document/cons_doc_LAW_122864/.

38 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/.

39 Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05 декабря 2016 г. № 646 // СПС «КонсультантПлюс. URL: http://www.consultant.ru/ ocument t/cons_doc_LAW_ 208191/4dbff9722e14f63a309bce4c2ad3d12cc2e85f10/.

40 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_381999/9bbf31c7586971ae3 d 3076bfb49080d41d6c4484.

41 О Стратегии национальной безопасности Российской Федерации до 2020 года: Указ Президента РФ от 12 мая 2009 г. № 537 (ред. от 01 июля 2014) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/ cons_doc_LAW_87685/.

42 О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 31 декабря 2015 г. № 683 // СПС «КонсультантПлюс».

URL: http://www.consultant.ru/document/cons_doc_LAW_191669/.

43 О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02 июля 2021 г. № 400 // СПС «КосультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_389271/.

44 Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_208191/.

45 Об утверждении Концепции внешней политики Российской Федерации: Указ Президента РФ от 30 ноября 2016 г. № 640 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_207990/.

46 О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы: Указ Президента РФ от 09 мая 2017 г. № 203 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_ 216363/.

47 Доктрина информационной безопасности Российской Федерации, утв. Президентом РФ 09 сентября 2000 г. № Пр-1895 // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LA W_28679/.

48 О единой автоматизированной информационной системе «Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено (вместе с "Правилами создания, формирования и ведения единой автоматизированной информационной системы "Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети "Интернет" и сетевых адресов, позволяющих идентифицировать сайты в информационно-

телекоммуникационной сети "Интернет", содержащие информацию, распространение которой в Российской Федерации запрещено", "Правилами принятия уполномоченными Правительством Российской Федерации федеральными органами исполнительной власти решений в отношении отдельных видов информации и материалов, распространяемых посредством информационно-телекоммуникационной сети "Интернет", распространение которых в Российской Федерации запрещено»): постановление Правительства РФ от 26 октября 2012 г. № 1101 (ред. от 29 апреля 2023) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_207990/.

49 Об утверждении Правил централизованного управления сетью связи общего пользования: постановление Правительства РФ от 12 февраля 2020 г. № 127 (ред. от 17 декабря 2021 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/c ons_doc_LAW_345574/.

50 Об утверждении правил оказания телематических услуг связи: постановление Правительства Российской Федерации от 31 декабря 2021 г. № 2607 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_406278/.

51 Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: постановление Правительства РФ от 17 февраля 2018 г. № 162 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document /cons_doc_LAW_291398/.

52 Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (вместе с «Правилами установки, эксплуатации и модернизации в сети связи оператора связи технических средств

противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования»): постановление Правительства РФ от 12 февраля 2020 г. № 126 (ред. от 28 мая 2022 г.) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/ document/cons_doc_ LAW_345571/.

53 Об утверждении технических условий установки технических средств противодействия угрозам, а также требований к сетям связи при использовании технических средств противодействия угрозам: приказ Роскомнадзора от 31 июля 2019 г. № 228 (зарегистрировано в Минюсте России 11 сентября 2019 г. № 55886) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_ 43224/.

54 Об утверждении Требований к порядку пропуска трафика в сетях передачи данных: приказ Минцифры России от 26 января 2022 г. № 44 (зарегистрировано в Минюсте России 28 февраля 2022 г. № 67538) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_ LAW_410516/.

55 Национальный стандарт Российской Федерации защита информации основные термины и определения: ГОСТ от 01 февраля 2008 г. Р 50922–2006 // СПС «КонсультантПлюс». URL: https://www.consultant.ru /cons/cgi/online.cgi?req=doc&base=OTN&n=25219#H6bMXrTwfRTQ5b4E2.

56 Оборудование периферийное систем обработки информации. Термины и определения: ГОСТ 25868–91 от 01 января 1993 г. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req= doc&base=OTN&n=9605#n9PbyZT2TCEk9pl21.

57 Системы обработки информации. Термины и определения: ГОСТ 15971–90 от 01 января 1992 г. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9Pb yZT2TCEk9pl21.

58 Передача данных. Термины и определения: ГОСТ 17657–79 // СПС

«КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZT2TCEk9pl21.

59 Информационно-коммуникационные технологии в образовании. Термины и определения: ГОСТ Р 52653–2006 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZT2TCEk9 pl21.

60 Передача данных. Термины и определения: ГОСТ 17657–79 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZT2TCEk9pl21.

61 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения: ГОСТ Р 53114–2008 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=9605#n9PbyZ T2TCEk9pl21.

62 Судебная компьютерно-техническая экспертиза. Термины и определения: ГОСТ Р 57429–2017: утв. и введен в действие 28 марта 2017 г. // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=OTN&n=25219#4eBizZTc1RID6We8.

1.2 Международные правовые акты

63 Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС КонсультантПлюс. URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#A4SN09UKowzg5kTu.

64 Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=13526#s6sltZT8ojzV24w91.

65 О защите физических лиц при автоматизированной обработке персональных данных Конвенция (заключена в г. Страсбурге 28 января 1981

г.) (вместе с Поправками к Конвенции о защите физических лиц при автоматизированной обработке персональных данных (СДСЕ № 108), позволяющими присоединение европейских сообществ, принятыми Комитетом Министров в Страсбурге 15 июня 1999 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_121499/.

66 Конвенция Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях: проект от 29 июня 2021 г. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/ Comments/RF_28_July_2021_-_R.pdf.

67 Право на неприкосновенность личной жизни в цифровой век: Резолюция, принятая Генеральной Ассамблеей 18 декабря 2013 г. A/68/456/Add.2 //ООН URL: https://www.un.org/ru/ga/third/68/third_res.shtml.

68 Резолюция ГА ООН A/RES/53/70 от 4 декабря 1998 г. URL: https://documentsddsny.un.org/doc/UNDOC/GEN/N99/760/05/PDF/N9976005.pdf?OpenElement.

69 Окинавская хартия глобального информационного общества от 21 июля 2000 года // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=8382#AuSltZTJodXDwttG.

70 Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (вместе с <Перечнями основных понятий и видов угроз, их источников и признаков>) (заключено в г. Екатеринбурге 16 июня 2009 г.) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=INT&n=51984#Kf6mtZTeq Mca dQ9Z1.

71 Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (ратифицировано Федеральным законом от 01 июля 2021 № 237-ФЗ) // СПС «КонсультантПлюс». http://www.consultant.ru/

document/cons_doc_LAW_388782/.

1.3 Памятники отечественного права

72 Конституция (Основной закон) Союза Советских Социалистических Республик (утверждена постановлением Чрезвычайного VIII Съезда Советов Союза Советских Социалистических Республик от 5 декабря 1936 г.) // СПС «Гарант». URL: https://constitution.garant.ru/history/ussr-rsfsr/1936/. Утратил силу.

73 Соглашение между Правительствами Союза Советских Социалистических Республик, Соединенных Штатов Америки и Соединенного Королевства Великобритании и Северной Ирландии и Временным Правительством Французской Республики о судебном преследовании и наказании главных военных преступников европейских стран оси 8 августа 1945 года URL: https://docs.cntd.ru/document/901737882.

74 Основы уголовного судопроизводства Союза ССР и союзных республик от 25 декабря 1958 г. // Ведомости Верховного Совета СССР. 1959. № 1. Утратил силу.

75 Об информации, информатизации и защите информации от 20.02.1995 г. № 24-ФЗ Федеральный Закон // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_ 5887/. Утратил силу.

76 О правовой охране программ для электронных вычислительных машин и баз данных Закон РФ от 23.09.1992 № 3523–1 (ред. от 02.02.2006) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document /cons_doc_LAW_1007/. Утратил силу.

77 О безопасности Закон РФ от 5 марта 1992 г. № 2446-I (с изменениями и дополнениями) // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_376/. Утратил силу.

78 Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ от 9 сентября 2000 г. № Пр-1895) (утратила силу) // СПС

«КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_28679/.

1.4 Современное зарубежное законодательство

79 Уголовный кодекс Китая / под ред. А.И. Коробеева и А.И. Чучаева, пер. с кит. Хуан Даосю. М., 2017. 256 с.

80 Уголовное уложение Федеративной Республики Германия – Strafgesetzbuch (StGB) (пер. П.В. Головненкова). URL: https://www.uni-potsdam.de/fileadmin/projects/lshellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf.

81 Уголовный кодекс Французской Республики. URL: https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006149839/#LEGISCTA000006149839.

82 Уголовный кодекс Республики Узбекистан (утвержден Законом Республики Узбекистан от 22 сентября 1994 года № 2012-XII) (ред. от 21 февраля 2024 г.). URL: https://online.zakon.kz/Document/?doc_id=30421110.

83 Закон о следственных полномочиях Великобритании от 29 ноября 2016 года. URL: https://www.legislation.gov.uk/ukpga/2016/25 /introduction. (Дата обращения 13.01.2024).

84 Закон о связи Великобритании от 17 июля 2003 года. URL: https://www.legislation.gov.uk/ukpga/2003/21/section/404. (Дата обращения 13.01.2024).

85 Закон о телекоммуникационной безопасности Великобритании от 17 ноября 2021 года. URL: https://www.legislation.gov.uk/ukpga/2021/31 /introduction/enacted.

86 Закон об электронном правительстве США. 2002. URL: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf.

87 Закон об электронном правительстве США. Раздел 3.

Информационная безопасность. 2002. URL: https://www.congress.gov/107/plaws/publ347/PLAW-107publ347.pdf.

88 Закон об электронном правительстве США. Раздел V. Конфиденциальная информация защита и статистическая эффективность. 2002. URL: https://georgewbush-whitehouse.archives.gov/omb/inforeg/cipsea/cipsea_statute.pdf.

89 Стратегия национальной кибербезопасности США. Сентябрь 2018 г. // URL: https://d-russia.ru/wp-content/uploads/2019/01/National-Cyber-Strategy_ USA_2018.pdf.

2 Судебная практика и статистические материалы

90 Об отказе в принятии к рассмотрению жалобы гражданина Супруна Михаила Николаевича на нарушение его конституционных прав статьей 137 Уголовного кодекса Российской Федерации: определение Конституционного Суда РФ от 28 июня 2012 № 1253-О // СПС «Гарант». URL: https://www.gara nt.ru/products/ipo/prime/doc/70105530/.

91 О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: постановление Пленума Верховного Суда РФ от 15 декабря 2022 № 37 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_434573/.

92 О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.[1], 139, 144.[1], 145, 145.[1] Уголовного кодекса Российской Федерации): постановление Пленума Верховного Суда РФ от 25 декабря 2018 № 46 // СПС «КонсультантПлюс». URL: http://www.consultant.ru/document/cons_doc_LAW_ 314616/.

93 О судебной практике по делам о мошенничестве, присвоении и растрате: постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_ 164858/.

94 Определение суда кассационной инстанции. Верховный Суд Российской Федерации. №49-УД23-21-А4, г. Москва, 20 июля 2023 г. URL: https://vsrf.r u/stor_pd f.php?id=2269520.

95 Приговор Саровского городского суда Нижегородской области № 1–167/2019 URL: https://sarovsky-nnov.sudrf.ru/modules.php?name=sud_delo&name_op=case&case_id=11412729&case_uid=d45ac732-0fab-45e1-b96934e877aad8dd&delo_id=1540006&case_type=0&new=0&srv_num=1.

96 Приговор Симоновского районного суда от 23 ноября 2020 г. № 1–285/2020 URL: https://mos-gorsud.ru/rs/nagatinskij/services/cases/criminal/details/4b008252-322c-46af-8a5a-0c2d2d4d5bc0.

97 Приговор Судакского городского суда Республики Крым от 07 мая 2018 г. URL: https://sudak-—–m.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=3168813&delo_id=1540006&new=0&text_number=1.

98 Приговор Кировского районного суда, г. Екатеринбург. Дело № 1–1/2022 (1-1/2021; 1-3/2020; 1-52/2019; 1-650/2018) URL: http://kirovsky.svd.sudrf.ru/modules.php?name=modsearch&text=&doSearch=%CD%E0%E9%F2%E8.

99 Приговор Свердловского районного суда от 2 августа 2013 г., № 1-493/2013 г. Красноярск URL: https://sudact.ru/regular/doc/E94OlaeV9h5q/?regulartxt=&regularcase_doc=%E2%84%961493%2F2013&regularlawchunkinfo=&regulardate_from=&regulardate_to=&regularworkflow_stage=&regulararea=&regularcourt=%29&regularjudge=&_=1679259851602.

100 Приговор Кировского районного суда г. Красноярск от 24.03.2017 г. № 1–171/2017. URL: https://kirovsk-—–k.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=18196178&delo_id=1540006&new=

0&text_number=1.

101 Приговор Бабушкинского районного суда ч. 1 ст. 272 УК РФ № 01-0656/2015 URL// https://mos-gorsud.ru/rs/babushkinskij/servicescases/c riminal/details/bac33fad-68c7-4d0c-87e9ad6d61317287?respondent=%D0%A8%D0%B5%D1%81%D1%82%D0%B0%D0%BA%D0%BE%D0%B2+%D0%93%D0%9F.

102 Приговор Ленинского районного суда от 11 мая 2017 г. по делу № 1–282/2017. URL: https://sudact.ru/regular/doc/bfZ4kLZF3mNg/.

103 Статистика и аналитика МВД России. URL: https://xn—b1aew.xn—p1ai/reports/item/16053092/.

104 Статистика и аналитика МВД России. URL: https://xn—b1aew.xn—p1ai/reports/item/19412450/.

105 Статистика и аналитика МВД России. URL: https://xn—b1aew.xn—p1ai/reports/item/22678184/.

106 Статистика и аналитика МВД России. URL: https://xn—b1aew.xn—p1ai/folder/101762.

2 Монографии, учебные пособия, учебники, комментарии

107 Артемов В.Ю., Власов И.С., Голованова Н.А. и др. Новые направления развития уголовного законодательства в зарубежных государствах: сравнительно-правовое исследование: монография. М. ООО «Юридическая фирма «Контакт», 2019. 642 с.

108 Борзенкова Г.Н. Комиссарова В.С. Курс уголовного права: в 5 т. Т. 4 / под ред. Г.Н. Борзенкова, В.С. Комиссарова. М.: Зерцало, 2002. 672 с.

109 Бриллиантов А.В. Комментарий к Уголовному кодексу Российской Федерации (постатейный): в 2 т. / 2 изд. М.: Проспект, 2016. Т. 1. 701 с.

110 Волеводз А.Г. Противодействие компьютерным преступлениям. М.: Юрлитинформ, 2002. 496 с.

111 Волков Ю.В. Информационное право. Информация как правовая

категория: учебное пособие для вузов. 2-е изд. М.: Юрайт. 2023 г. 109 с.

112 Винер Н. Кибернетика и общество. М.: Иностранная литература, 1958. 199 с.

113 Галяшина Е.И, Никишин В.Д. и др. Фейковизация как средство информационной войны в интернет-медиа: науч.-практ. пос. М.: Блок-Принт, 2023. 144 с.

114 Глушков В.М. Амосов Н.М. Артеменко И.А. Энциклопедия кибернетики. Киев: Главная редакция украинской советской энциклопедии, 1974. 608 с.

115 Грачева Ю.В. Риски цифровизации: виды, характеристика, уголовно-правовая оценка: монография. М.: Проспект, 2022. 270 с.

116 Дремлюга Р.И. Интернет-преступность: монография / под ред. В.Г. Дроздова. Владивосток: Изд-во Дальневост. ун-та, 2008. 240 с.

117 Ефремова М.А. Уголовная ответственность за преступления, совершаемые с использованием информационно-коммуникационных технологий: монография. М.: Юрлитинформ, 2015. 200 с.

118 Жижина М.В., Завьялова Д.В. Расследование преступлений в сфере компьютерной информации в Российской Федерации и зарубежных странах: монография. М.: Проспект, 2022. 136 с.

119 Комментарий к Уголовному кодексу Российской Федерации (научно-практический) / под ред. А.И. Чучаева. М.: Проспект, 2022. 1349 с.

120 Корабельников С.М. Уголовно-правовая защита информационных отношений: учеб. пос. М.: Проспект, 2022. 96 с.

121 Крутских А.В. Зиновьева Е.С. Международная информационная безопасность: подходы России. М.: МГИМО, 2021. 48 с.

122 Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пос. М.: Горячая линия – Телеком, 2004. 280 с.

123 Малинин В.В. Энциклопедия уголовного права. Т. 14. Преступления против свободы, чести и достоинства личности. СПб.: ГКА,

2010. 628 с.

124 Морозов И.Л. Политический экстремизм: особенности эволюции при переходе от индустриального общества к информационному: монография. Волгоград: Перемена, 2007. 457 с.

125 Наумов А.В. Российское уголовное право: Общая часть: курс лекций. М.: Издательство БЕК, 2000. 560 с.

126 Овчинский В.С. Криминология цифрового мира: учебник. М.: Инфра-М, 2018. 352 с.

127 Попов А.Н. Преступления в сфере компьютерной информации: учеб. пос. СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 69 с.

128 Рарог А.И. Уголовное право России. Части Общая и Особенная: учебник 10-е изд., перераб. и доп. М.: Проспект, 2019. 841 с.

129 Российское уголовное право. Общая часть: учебник / под ред. В.П. Коняхина и М.Л. Прохоровой. М.: КОНТРАКТ, 2014. 560 с.

130 Русскевич Е.А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. М.: ИНФРА-М, 2020. 351 с.

131 Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использование информационно-коммуникационных технологий: учеб. пос. М.: ИНФРА-М, 2018. 115 с.

132 Сперанский М.М. План государственного преобразования графа М.М. Сперанского (введение к уложению государственных законов 1809 г.) с приложением «Записки об устройстве судебных и правительственных учреждений в России» (1803 г.), статей «О государственных установлениях», «О крепостных людях» и Пермского письма к императору Александру // СПС «Гарант». URL: https://constitution.garant.ru/history/act1600-1918/3848894/. 359 с.

133 Степанов О.А. Противодействие кибертерроризму в цифровую эпоху. монография. М.: Юрайт, 2020. 103 с.

134 Шеннон К. Работы по теории информации и кибернетике.

М.: Иностранная литература, 1963. 832 с.

135 Юрченко И.А. Преступления против информационной безопасности: учебное пособие. М.: Проспект, 2022. 208 с.

3 Научные статьи

136 Акопов Г.Л. Хактивизм – угроза информационной безопасности в информационном социуме // Государственное и муниципальное управление. Ученые записки. 2015. № 3. С 195-199.

137 Антонов А.Г., Зорина Е.А., Крюков Д.В. К вопросу об общественной опасности неправомерного доступа к компьютерной информации // Вестн. Том. гос. ун-та. Право. 2022. № 44. С. 5-16.

138 Бутова Л.И. Характеристика и сущность киберпреступлений // Алтайский юридический вестник. 2016. № 3 (15). С. 28-31.

139 Буз С.И. Киберпреступления: понятие, сущность и общая характеристика // Юристъ – Правоведъ. 2019. №4 (91). С. 78-82.

140 Бражник С.Д. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК РФ): Мифы, реальность, перспективы; Прогресс и преемственность в российском уголовном праве (к 95-летию УК РСФСР 1926 и 25-летию УК РФ 1996 г.) материалы Всероссийской научно-практической конференции с международным участием / отв. ред. В.П. Коняхин и М.Л. Прохорова. Краснодар: Кубанский государственный университет. 2021. С. 526-540.

141 Валеев А.Х. Борьба с проявлением экстремизма в сети Интернет // Бизнес в законе. 2011. № 6. С. 125-127.

142 Ван Гуанлун Уголовно-правовое регулирование противодействия киберпреступности в Китае: состояние, тенденции и недостатки // Вестник СПбГУ. Серия 14. Право. 2022. №3. С. 661-677.

143 Вильданов Р.Р., Кутушева Э.Н. Система государственного регулирования интернета в Китайской Народной Республике // Вестник

УГНТУ. Наука, образование, экономика. Серия: Экономика. 2021. № 3 (37). С. 115-122.

144 Гребенкин Ф.Б. Некоторые проблемные вопросы объективных признаков состава преступления, предусмотренного ст. 273 УК РФ // Вестник гуманитарного образования. 2017. № 2. С. 61-67.

145 Данельян А.А. Международно-правовое регулирование киберпространства // Образование и право. 2020. № 1. С. 82-89.

146 Дремлюга Р.И. Критическая информационная инфраструктура как предмет посягательства в законодательстве зарубежных стран // Журнал зарубежного законодательства и сравнительного правоведения. 2022. Т. 18. № 3. С. 27-36.

147 Дремлюга Р.И., Коробеев А.И. Ответственность за создание, использование и распространение вредоносных компьютерных программ по законодательству зарубежных стран // Российский следователь. 2022. № 5. С. 67-71.

148 Дремлюга Р.И., Коробеев А.И. Преступные посягательства на системы искусственного интеллекта: уголовно-правовая характеристика // Всероссийский криминологический журнал. 2023. Т, 17. № 1. С. 5-12.

149 Дремлюга Р.И., Крипакова А. В. Преступления в виртуальной реальности: миф или реальность? // Актуальные проблемы российского права. 2019. № 3 (100). С. 161-169.

150 Дремлюга Р.И., Зотов С.С., Павлинская В.Ю. критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. № 2. С. 130-139.

151 Евдокимов К.Н. Актуальные вопросы совершенствования уголовно-правовых средств борьбы с компьютерными преступлениями // Вестник Казанского юридического института МВД России. 2016. № 2 (24). С. 62-66.

152 Евдокимов К.Н. Актуальные вопросы определения объекта

преступного посягательства при нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) // Ученые записки Крымского федерального университета имени В. И. Вернадского. Юридические науки. 2018. № 4. С. 187-195.

153 Ефремова И.А., Смушкин А.Б., Донченко А.Г., Матушкин П.А. Киберпространство как новая среда преступности // Вестн. Том. гос. ун-та. 2021. № 472. С. 248-256.

154 Ефремова М.А. К вопросу об уголовной ответственности за создание, распространение и использование вредоносных компьютерных программ// Информационное право. 2015. № 3. С. 12-16.

155 Ефремова М.А. Международно-правовые основы уголовно-правовой охраны информационной безопасности // Правосудие. 2020. № 1. С. 82-98.

156 Закупень Т.В. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ // Информационные ресурсы России. 2009. № 4. С. 28-34.

157 Звягинцев М.Н. О необходимости нормативного правового акта «О системе правовых актов» // Источники права: проблемы создания, систематизации и реализации: межвуз. сб. ст. / под ред. В.Я. Музюкина, В.В. Сорокина. Барнаул: АлтГУ. 2007. С. 43-46.

158 Зигмунт О.А., Петровский А.В. Кибер и интернет-преступность в Германии и России: возможности сравнительного исследования // Юридическая наука и правоохранительная практика. 2015. № 4 (34). С. 180-188.

159 Карпова Д.Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46-50.

160 Карабанова Е.Н. Понятие объекта преступления в современном уголовном праве // Журнал российского права. 2018. № 6 (258). С. 69-77.

161 Карташкин В.А., Быков И.П. Права человека и информационный экстремизм // Вестник РУДН. Серия: Социология. 2021. № 3. С. 580-589.

162 Коняхин, В.П. Компьютерные преступления: компаративистский анализ // Научно-технологическое обеспечение агропромышленного комплекса России: проблемы и решения: Сборник тезисов по материалам III Национальной конференции, Краснодар, 27–28 марта 2019 г. Краснодар: Кубанский государственный аграрный университет имени И.Т. Трубилина, 2019. С. 184.

163 Коротких Н.Н., Останин М.Д. К вопросу о соотношении понятий «преступление в сфере компьютерной информации» и «компьютерное преступление» // Азиатско-Тихоокеанский регион: экономика, политика, право. 2018. № 3. С. 69-77.

164 Кочкина Э.Л. Определение понятия «киберпреступление». Отдельные виды киберпреступлений // Сибирские уголовно-процессуальные и криминалистические чтения. 2017. № 3 (17). С. 162-169.

165 Кузнецов А.П., Гарипова Н.В. Проблемы определения непосредственного объекта в преступлениях в сфере компьютерной информации / А.П. Кузнецов, Н.В. Гарипова // Следователь, 2008. № 7. С. 5-7.

166 Куфлева В.Н., Литовченко А.И. Проблемы квалификации преступлений, связанных с использованием шифрования информации и обеспечением анонимности в сети интернет // Общество: политика, экономика, право. 2021. № 9 (98). С. 80-83.

167 Кулешова Г.П., Капитонова Е.А., Романовский Г.Б. Правовые основы противодействия кибертерроризму в России и за рубежом с позиции общественно-политического измерения // Всероссийский криминологический журнал. 2020. № 1. С. 156-165.

168 Кучина Я.О. Некоторые особенности объекта преступления в ст. 274^1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» // Проблемы борьбы с преступностью в условиях цифровизации: теория и практика: сб. ст. Междунар. науч.-практ. конф. Барнаул, 2020. С. 60-63.

169 Лексютина Я.В. Политика китайского руководства в вопросах

контроля и регулирования Интернета // Общество и государство в Китае. 2015. № 1. С. 202-212.

170 Липинский Д.А., Евдокимов К.Н. Политические причины как современные факторы эволюции компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2015. № 1. С. 101-110.

171 Лихачев Н.А. Нематериальное пространство как новая форма места совершения преступления: доктринальный аспект // Юридические исследования. 2024. № 4. С. 1-8.

172 Лихачев Н.А. Неправомерный доступ к компьютерной информации: направления оптимизации состава // Гуманитарные, социально-экономические и общественные науки. 2023. № 4. С. 153-157.

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

174 Лихачев Н.А. Современная уголовная политика Российской Федерации в сфере обеспечения информационной безопасности 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.)» (Кубанский государственный университет, г. Краснодар, 28-29.05.2021 г.). С. 637-642.

175 Лихачев Н.А. «Уголовно-правовые меры противодействия преступлениям, связанным с посягательствами на персональные данные граждан» Международная научно-практическая конференция «Уголовно-правовые меры противодействия служебным, экономическим и иным преступлениям: современное состояние и пути оптимизации» (юридический факультет Ярославского государственного университета им. П.Г. Демидова, г. Ярославль, 30.09-1.10.2022 г.). С. 83-87.

176 Лихачев Н.А. Международное уголовно-правовое

противодействие преступлениям в сфере информационной безопасности // Вопросы российского и международного права. 2023. №4. С. 438-443.

177 Ляпунов Ю.И. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 8-15.

178 Мазуров В.А., Потапов Д.П., Сорокин В.В. Компьютерные преступления: анализ уголовного законодательства США и Германии // Известия АлтГУ. 2005. № 2. С. 59-66.

179 Маслакова Е.А. Лица, совершающие преступления в сфере информационных технологий: криминологическая характеристика // Среднерусский вестник общественных наук. 2014. № 1 (31). С. 114-121.

180 Манойло А.В. «Фейковые новости» как угроза национальной безопасности и инструмент информационного управления // Вестник Московского университета. Серия 12. Политические науки. 2019. № 2. С. 37-45.

181 Маякова А.С., Шелепова С.А. Компьютерные преступления: отдельные вопросы квалификации // Проблемы экономики и юридической практики. 2017. № 6. С. 191-194.

182 Мирошников Б.Н. Перспективы международного сотрудничества в рамках Конвенции о киберпреступности // Национальные интересы: приоритеты и безопасность. 2007. № 6. С. 46-48.

183 Мицкевич А.Ф., Суслопаров А.В. Понятие компьютерной информации по российскому и зарубежному уголовному праву // Пробелы в российском законодательстве. 2010. № 2. С. 206-209.

184 Наумов В.Б., Архипов В.В. Понятие персональных данных: интерпретация в условиях развития информационно-телекоммуникационных технологий // Российский юридический журнал. 2016. № 2. С. 186-196.

185 Некрасова Е.В. Информационный аспект экстремизма и терроризма и деструктивные тенденции в сми // Вестник РУДН. Серия: Социология. 2013. №1. С. 57-66.

186 Номоконов В.А., Тропина Т.Л. Киберпреступность как новая

криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 24. С. 45-55.

187 Пелевина А.В. Общая характеристика преступлений в сфере компьютерной информации // Пробелы в российском законодательстве. 2015. № 4. С. 209-211.

188 Пелевина А.В. Ответственность за компьютерные преступления в романо-германской правовой системе // Пробелы в российском законодательстве. 2016. № 3. С. 76-79.

189 Протасевич А.А., Зверянская Л.П. Борьба с киберпреступностью как актуальная задача современной науки // Всероссийский криминологический журнал. 2011. № 3. С. 28-33.

190 Прохоров Л.А., Бондарь Е.В. Уголовная ответственность за фальсификацию исторических сведений и искажение фактов о роли СССР в победе над германским фашизмом в Великой Отечественной войне // Гуманитарные, социально-экономические и общественные науки. 2018. № 9. С. 135-139.

191 Рарог А.И. Правовое значение разъяснений Пленума Верховного Суда РФ // Государство и право. 2001. № 2. С. 51-57.

192 Родивилин И.П. Особенности характеристики состояния и структуры преступлений в сфере обращения охраняемой законом информации в современный период в Российской Федерации // Вестник Восточно-Сибирского института МВД России. 2020. № 4 (95). С. 64-72.

193 Романов И.В. Понятие киберпреступлений и его значение для расследования // Сибирские уголовно-процессуальные и криминалистические чтения. 2016. № 5 (13). С. 105-109.

194 Ромашкина Н.П. Глобальные военно-политические проблемы международной информационной безопасности: тенденции, угрозы, перспективы // Вопросы кибербезопасности. 2019. № 1 (29). С. 2-9.

195 Россинская Е.Р., Рядовский И.А. Концепция вредоносных программ как способов совершения компьютерных преступлений:

классификации и технологии противоправного использования // Всероссийский криминологический журнал. 2020. № 5. С. 699-709.

196 Семенова В.Г., Петриченко Е.А. Информация: история понятия, его настоящее и будущее // Известия вузов. Северо-Кавказский регион. Серия: Общественные науки. 2022. №1 (213). С. 16-26.

197 Сидорова Т.Ю. Международная информационная безопасность: правовые аспекты и деятельность ООН // Сибирский юридический вестник. 2020. № 3 (90). С. 103-108.

198 Соловьев В.С. Криминологическая типология механизмов совершения преступлений с использованием информационно-телекоммуникационных технологий // Вестник Краснодарского университета МВД России. 2021. № 4 (54). С. 50-57.

199 Соловьев В.С., Осипенко А.Л. Формы проявления организованной преступности в информационно-телекоммуникационной среде // Уголовная политика и культура противодействия преступности: материалы Международной научно-практической конференции памяти профессора В.Е. Квашиса (г. Краснодар, 29 сентября 2023 г.). Краснодар: Краснодарский университет МВД России, 2023. С. 263-275.

200 Стяжкина С.А. Уголовно-правовые особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (статья 274 УК РФ) // Вестник Удмуртского университета. Серия «Экономика и право». 2021. №3. С. 489-496.

201 Талимончик В.П. Информационная безопасность в контексте всеобъемлющей системы международной безопасности // Правоведение. 2008. № 2. С. 105-116.

202 Талапина Э.В. Защита персональных данных в цифровую эпоху: российское право в Европейском контексте // Труды Института государства и права РАН. 2018. № 5. С. 117-150.

203 Тимошков С.Г. Кибератака как современная форма совершения

акта агрессии // Вестник РГГУ. Серия «Экономика. Управление. Право». 2017. №1 (7). С. 127-135.

204 Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99-106.

205 Цимбал В.Н., Клюев С.Г. Понятие киберпреступления и его содержательная часть// Вестник Московского университета МВД России. 2021. № 1. С. 129-132.

206 Харламова А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации // Вестник Уральского юридического института МВД России. 2020. № 2. С. 162-167.

207 Шинкарецкая Г.Г., Берман А.М. Кибератаки – противоправное использование цифровых технологий // Международное право. 2022. №1. С. 40-50.

208 Шульга А.В., Галиакбаров Р.Р. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК РФ) // Гуманитарные, социально-экономические и общественные науки. 2018. № 5. С. 86-92.

209 Энгельгардт А.А. Компьютерная информация как предмет преступления, предусмотренного статьей 273 Уголовного кодекса Российской Федерации // Право. Журнал Высшей школы экономики. 2014. № 4. С. 136-145.

210 Якимова Е.М., Нарутто С.В. Международное сотрудничество в борьбе с киберпреступностью // Криминологический журнал Байкальского государственного университета экономики и права. 2016. Т. 10, № 2. С. 369-378.

211 Collin B.C. The Future of Cyber Terrorism // Crime & Justice International. 1997. Vol. 13, no. 2. March. P. 15-18.

212 Clarke Richard A., Knake Robert K. Cyber war: the next threat to

national security and what to do about it. OUP, 2010. P. 6.

213 Cyberterrorism: Hype and Reality Maura Conway Dublin City University. 2007. URL// https://doras.dcu.ie/501/1/cybert_hype_reality_2007.pdf.

214 Denning D.E. A View of Cyberterrorism Five Years Later // Internet Security: Hacking, Counterhacking, and Society / ed. by K. Himma. Sudbury, MA, 2006. P. 123-141.

215 Global Business Data Platform Statista. URL: https://www.statista.com/statistics/631151/worldwide-data-collected-by-smart-buildings/. P. 43-48.

216 Kim S.H. A comparative study of cyberattacks / Seung Hyun Kim, Qiu-Hong Wang, Johannes B. Ullrich // Communications of the ACM. 2012. Vol. 55, iss. 3. P. 66-73.

217 National cybersecurity strategy of USA, march 2023. URL: http://pentagonus.ru/doc/ National_Cybersecurity_Strategy_03_2023.pdf. P. 14-20.

218 Navarria G. China: the Party, the Internet, and power as shared weakness // Global Change, Peace and Security. 2016. Vol. 29. P. 1-20.

219 Schroetter M Invariaiice as a Tool for Ontology of Information // Information. 2016. № 7-1 (11). P. 2-20.

220 The Business of Hacking Business innovation meets the business of hacking. Hewlett Packard Enterprise. 2016. C. 7. URL: https://static.politico.com/b9/5 5/4e3ce4cc41d88401e264dcacc35c/hpe-security-research-business-of-hacking-may-2016.pdf. P. 56-60.

221 Walter Laqueur, The New Terrorism: Fanaticism and the Arms of Mass Destruction. Oxford: Oxford University Press, 1999. P. 254.

222 Yu, Zhigang. 2010a. “Cybercrime and China’s Criminal Law response”. Zhongguo Shehuikexue 3. P. 109-126.

5 Диссертации, авторефераты диссертаций

223 Арапова Н.П. Социально-информациологический подход в теории информационных войн: дис. ... канд. полит. наук. М., 2003. 181 с.

224 Асланян Р.Г. Информация как предмет и средство совершения преступлений в сфере экономической деятельности: автореф. дис. ... канд. юрид. наук. Краснодар, 2016. 21 с.

225 Бегишев И.Р. Понятие и виды преступлений в сфере обращения цифровой информации: автореф. дис. ... канд. юрид. наук. К., 2017. 31 с.

226 Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. ... канд. юрид. наук. Казань, 2017. 243 с.

227 Губарев А.Б. Информационные войны как объект политологического исследования: дис. ... канд. полит. наук. Уссурийск, 2005. 170 с.

228 Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации (по материалам Восточно-Сибирского округа): автореф дис. канд. юрид. наук. Иркутск, 2006. 203 с.

229 Ефремова М.А. Уголовно-правовая охрана информационной безопасности: дис. … д-ра. юрид. наук: М., 2018. 427 с.

230 Калмыков Д.А. Информационная безопасность: понятие, место в системе уголовного законодательства РФ, проблемы правовой охраны: автореф. дис. … канд. юрид. наук. Казань, 2005. 219 с.

231 Касенова М.Б. Правовое регулирование трансграничного функционирования и использования Интернета: автореф. дис. … д-ра юрид. наук. М., 2016. 66 с.

232 Лопатин В.Н. Информационная безопасность России: автореф. дис. … д-ра юрид. наук., СПб., 2000. 433 с.

233 Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: дис. … канд. юрид. наук. М., 2007. 186 с.

234 Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. … канд.

юрид. наук. Орел, 2008. 198 с.

235 Разуваев В.Э. Правовые средства противостояния информационным войнам: дис. ... канд. юрид. наук. М., 2005. 174 с.

236 Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: автореф. дис. ... канд. юрид. наук. М., 1998. 161 с.

237 Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): дис. … д-ра юрид. наук. М., 2016. 389 с.

238 Упорников Р.В. Политико-правовые технологии противодействия информационному экстремизму в России: дис. … канд. юрид. наук. Ростов н/Д, 2007. 148 с.

239 Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений: дис. ... канд. юрид. наук. М., 2016. 249 с.

240 Шмарион В.И. Ответственность за преступления против чести и достоинства личности по российскому уголовному законодательству: дис. ... канд. юрид. наук. Ростов н/Д, 2001; 228 с.

241 Ягудин А.Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: дис. ... канд. юрид. наук. Казань, 2012. 208 с.

6 Энциклопедии, словари и справочники

242 Кузнецов С.А. Современный толковый словарь русского языка. М. Издательский дом Ридерз Дайджест. 2004. 958 с.

243 Ожегов С.И. Словарь русского языка: ок. 57000 слов / под ред. Н.Ю. Шведовой 13-е изд., испр. М.: Просвещение 1981. 604 с.

244 Семёнов А.В. Этимологический словарь русского языка.

«Русский язык от А до Я». М.: «ЮНВЕС», 2003 г. 704 с.

7 Интернет-ресурсы

245 Бельгиец покончил с собой после шести недель общения с чат-ботом // ТАСС. 29 марта 2023. URL: https://tass.ru/proisshestviya/17399117.

246 Вся статистика интернета на 2020 г. – цифры и тренды в мире и в России // Web Canape. 03.02.2020 г. URL: https:// www.web-canape.ru/business/internet- 2020-globalnaya-statistika-i-trendy/.

247 Видеообращение председателя Правительства РФ М.В. Мишустина к участникам 13-й Недели российского интернета – RIW 20/21. URL: http://government.ru/news/44012/.

248 В г. Тверь возбуждено уголовное дело по факту публичного распространения под видом достоверных сообщений заведомо ложной информации об обстоятельствах, представляющих угрозу жизни и безопасности граждан // Официальный сайт Следственного комитета Российской Федерации. URL: https://tver.sledcom.ru/news/item/1455217/.

249 Какие существуют типы вредоносных программ? // Официальный сайт Лаборатории Касперского. URL: https://www.kaspersky.ru/resource-center/threats/types-of-malware.

250 Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М.: Генеральная Прокуратура РФ, 2013. URL: https://epp.genproc.gov.ru/web/gprf/documents; Российская газета. 2017. 24 янв.

251 Послание Президента Российской Федерации Федеральному Собранию Российской Федерации 01 декабря 2016 г. URL: http://kremlin.ru/events/ president/ news/53379.

252 Пояснительная записка к проекту федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и

Уголовно-процессуальный кодекс Российской Федерации» // Официальный сайт Государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/130406-8.

253 Пояснительная записка к проекту Федерального закона «О внесении изменений в некоторые законодательные акты Российской Федерации» // Официальный сайт Государственной Думы РФ. URL: https://sozd.duma.gov.ru/bill/608767-7.

254 Сбербанк рассказал о раскрытой сети мошеннических колл-центров в Бердянске // RG RU. URL: https:// rg.ru/2022/06/03/sberbank-rasskazal-o-raskrytoj-setimoshennicheskih-koll-centrov-vberdianske.html?Msn=&.

255 Суд приговорил лидера хакерской группировки Lurk к 14 годам колонии, // РБК. Общество. 14 февраля 2022 г. URL: https://amp.rbc.ru/rbcnews/society/14/ 02/2022/620a1ecf9a79476a8b26419b.

256 Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций Российской Федерации. URL: https://rkn.gov.ru/news/rs c/news73728.htm.

257 ФСБ поручено создать антихакерскую систему // Вести. 21 января 2013 г. URL: http://www.vesti.ru/doc.html?id=1010793.

258 Число пользователей интернета в Китае к концу 2021 года превысило 1 млрд человек // ТАСС. URL: https://tass.ru/obschestvo/13855855.

259 37 процентов людей никогда не пользовались интернетом. Новости // URL: OOHURL//https://news.un.org/ru/story/2021/11/1414732.

Приложение 1

Предлагаемые редакции статей 272–274[1] 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.

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…

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…

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…

Приложение 2

Анкета для опроса следователей Министерства внутренних дел Российской Федерации (МВД России), Следственного комитета Российской Федерации (СК РФ), судей федеральных судов общей юрисдикции по теме исследования, посвященного проблематике противодействия преступлениям в сфере обеспечения информационной безопасности

Уважаемый респондент!

В рамках осуществляемого мной диссертационного исследования по теме: «Уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности: законодательный, правоприменительный и доктринальный аспекты» обращаюсь к Вам с просьбой ответить на вопросы, которые возникли в процессе ее изучения. Ответы, полученные от Вас, будут содействовать разработке доктринальных выводов и законодательных инициатив, направленных на совершенствование уголовно-правового противодействия преступлениям в сфере обеспечения информационной безопасности и защиты информации.

Прошу Вас ответить на предварительные вопросы

№	**Вопрос**	**Результат**
1	Ваш возраст а) от 20 до 30 лет; б) от 31 до 45 лет; в) от 45 лет.	а) 35 % б) 53 % в) 12 %
2	Занимаемая должность: а) следователь МВД России, СК РФ; б) судья федерального суда общей юрисдикции.	а) 68 % б) 32 %
3	Стаж работы в указанной должности: а) до 3 лет; б) от 3 до 10 лет; в) свыше 10 лет.	а) 20 % б) 68 % в) 12 %

4	Известно ли Вам, что из себя представляет уголовно-правовое противодействие преступлениям в сфере обеспечения информационной безопасности? а) знаю; б) не знаю; в) затрудняюсь ответить.	а) 70 % б) 12 % в) 18 %

Вопросы по теме исследования

№	Вопрос	Результат
1.	Как Вы считаете, необходима ли дополнительная криминализация деяний, связанных с процессом создания, хранения, обмена, распространения информации, с целью большего государственного контроля и защиты персональных данных граждан? А) да Б) нет В) затрудняюсь ответить	а) 68 % б) 13 % в) 19%
2.	Согласны ли Вы с тем, что совершение преступления с использованием информационно-телекоммуникационных технологий, в том числе сети «Интернет», обладает повышенной степенью общественной опасности в связи с особой трудностью выявления и пресечения подобного рода деяний на стадии приготовления, в том числе приискания орудий совершения преступления, а также сокрытия его следов? А) да Б) нет	а) 82 % б) 18 %
3.	Считаете ли Вы целесообразным рассматривать совершение преступления с использованием информационно-телекоммуникационных технологий, в том числе сети «Интернет», как квалифицирующий признак или обстоятельство, отягчающее наказание? А) да Б) нет	а) 72 % б) 28 %
4.	Как Вы считаете, можно ли отразить в российском уголовном законе следующее определение кибератаки – «противоправные действия по массовому воздействию на компьютеры, компьютерные сети и системы, их блокирование, повреждение, уничтожение, получение 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»? А) да Б) нет	 а) 75 % б) 25 %
5.	Согласны ли Вы с данным доктринальным определением информации как объекта уголовно-правовой охраны – «сведения конфиденциального характера, содержащие персональные данные или относящиеся к любой разновидности тайны, порядок допуска к которым, в том числе ознакомление с ними, их распространение, копирование, изменение, уничтожение, а также порядок и форма хранения подлежат императивному правовому регулированию, нарушение которого влечет привлечение к уголовной ответственности»? А) да Б) нет	 а) 81 % б) 19 %
6.	Согласны ли Вы с необходимостью криминализации в рамках ст. 272 УК РФ непосредственного ознакомления с информацией в ходе реализации преступного умысла на осуществление непосредственного доступа к ней? А) да Б) нет В) затрудняюсь ответить	 а) 79 % б) 12 % в) 9%
7.	Согласны ли Вы с предложением о необходимости криминализации неправомерного доступа к компьютерной информации, сопряженного с последующей трансграничной передачей компьютерной информации, содержащей персональные данные, и (или) трансграничным перемещением носителей, содержащих такие данные? А) да Б) нет В) затрудняюсь ответить	 а) 86 % б) 10 % в) 4%
8.	Согласны ли Вы с идеей, согласно которой киберпространство и информационное пространство следует рассматривать как специфическую криминальную среду со своей контркультурой, особенностями способов и средств совершения преступлений, которая влияет на степень общественной опасности, что в некоторых случаях законодателем уже фактически учтено (нормы Особенной части УК РФ, где совершение деяния в ИТС «Интернет» выделено в качестве квалифицирующего признака)?	

	А) да Б) нет В) затрудняюсь ответить	а) 73 % б) 10 % в) 16%
9.	Считаете ли Вы необходимым уточнение территориального принципа действия уголовного закона в пространстве путем определения соотношения киберпространства и информационного пространства через закрепление юрисдикции государства за его национальным сегментом ИТС «Интернет», распространив суверенитет за пределы материального мира и традиционного формата определения места в пределах границы государства? А) да Б) нет В) затрудняюсь ответить	 а) 69 % б) 10 % в) 21%
10.	Согласны ли Вы с необходимостью криминализации записи непубличных разговоров с последующей передачей ее третьим лицам, если указанные действия повлекли за собой наступление тяжких последствий, распространения компьютерной информации, полученной преступным путем, получения доступа к охраняемой законом информации посредством обмана и злоупотребления доверием? А) да Б) нет В) затрудняюсь ответить	 а) 76 % б) 13 % в) 11%

Благодарю за участие в опросе!