Негосударственное образовательное учреждение
организация высшего образования
«Российская академия адвокатуры и нотариата»

На правах рукописи

МАЛЫГИН Иван Игоревич

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ НЕПРАВОМЕРНОМУ ВОЗДЕЙСТВИЮ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

Специальность 5.1.4 — Уголовно-правовые науки

АВТОРЕФЕРАТ

диссертации на соискание ученой степени
кандидата юридических наук

Москва — 2023

Работа выполнена на кафедре адвокатуры и уголовно-правовых дисциплин негосударственного образовательного учреждения организации высшего образования «Российская академия адвокатуры и нотариата»

Научный руководитель: **Букалерова Людмила Александровна**, доктор юридических наук, профессор, профессор кафедры адвокатуры и уголовно-правовых дисциплин негосударственного образовательного учреждения организации высшего образования «Российская академия адвокатуры и нотариата»

Официальные оппоненты: **Серебренникова Анна Валерьевна,** доктор юридических наук, профессор кафедры уголовного права и криминологии федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова»

Ефремова Марина Александровна, доктор юридических наук, профессор кафедры уголовного права и криминологии Казанского института (филиала) федерального государственного бюджетного образовательного учреждения высшего образования «Всероссийский государственный университет юстиции (РПА Минюста России)»

Ведущая организация: Федеральное государственное бюджетное образовательное учреждение высшего образования «Уральский государственный юридический университет имени В.Ф. Яковлева»

Защита состоится «29» ноября 2023 года в 14.00 часов на заседании диссертационного совета 75.2.047.01, созданном на базе негосударственного образовательного учреждения организации высшего образования «Российская академия адвокатуры и нотариата», по адресу: 105120, г. Москва, Малый Полуярославский пер., д. 3/5, стр.1.

С диссертацией можно ознакомиться в Научной библиотеке и на официальном сайте негосударственного образовательного учреждения организации высшего образования «Российская академия адвокатуры и нотариата» по адресу https://raa.ru.

Автореферат разослан «__» _____ 2023 г.

Ученый секретарь
диссертационного совета Ю.Н. Богданова Ю.Н. Богданова

ВВЕДЕНИЕ

Актуальность темы диссертационного исследования. С каждым днем цифровизация общественной жизни, экономики и государственного управления становится все более всеохватывающим процессом, поскольку она позволяет добиться принципиального повышения эффективности в том или ином сегменте деятельности. Здесь эффективность необходимо понимать в самом широком смысле — как повышение качества деятельности, при котором желаемый результат достигается наиболее разумным способом (с наименьшими затратами ресурсов и времени). В экономике эффективность довольно легко измеряется увеличением доходности, общей производительности, снижением затрат и времени. В социальной сфере об эффективности цифровизации можно судить по тому, насколько она улучшает коммуникацию, обеспечивает реализацию прав и свобод человека, повышает социальную активность граждан и т. п. В результате информационно-коммуникационная инфраструктура приобретает значение «цифрового остова» государства. Негативное воздействие на такой каркас сопряжено с угрозой не всегда предсказуемых, но, как правило, весьма серьезных последствий.

С 1 января 2018 г. в отечественном уголовном законодательстве действует специальная норма — ст. 274[1] УК РФ[1] об ответственности за компьютерные атаки и иное неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (далее – КИИ)[2].

В доктрине уголовного права реализация данной законотворческой инициативы в целом была встречена позитивно, что весьма редкое явление в современных условиях. Зачастую курс законодателя на казуализацию уголовного

---

[1] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ : федер. закон : принят Гос. Думой Федер. Собр. Рос. Федерации 24 мая 1996 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 5 мая 1996 г. : по состоянию на 18 марта 2023 г. // Собр. законодательства Рос. Федерации. 1996. № 25, ст. 2954 ; Официальный интернет-портал правовой информации www.pravo.gov.ru, 18.03.2023.

[2] Федеральные законы от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и № 194-ФЗ «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"» : приняты Гос. Думой Федер. Собр. Рос. Федерации 12 июля 2017 г. : одобр. Советом Федерации Федер. Собр. Рос. Федерации 19 июля 2017 г. : вступили в законную силу с 1 янв. 2018 г. // Официальный интернет-портал правовой информации www.pravo.gov.ru, 26.07.2017.

закона научная общественность подвергает критике, справедливо ссылаясь на то, что это приводит к многочисленным сложностям на уровне правоприменения.

Однако, как свидетельствуют статистические данные, с самого момента закрепления норма показала свою востребованность. Так, по данным Министерства внутренних дел Российской Федерации (МВД России) в 2018 г. было зарегистрировано лишь одно преступление по ст. ст. 274[1] УК РФ, в 2019 г. — 4, в 2020 г. — 22, в 2021 г. — 159, в 2022 г. таких преступлений зарегистрировано уже 519 (рост на 226,41 %)[3]. Как известно, данные о регистрации преступлений далеко не всегда могут отражать реальную ситуацию в сфере противодействия преступности. Более показательны в этом отношении сведения о числе осуждений, которые в том числе позволяют оценить, насколько хорошо на практике понимается содержание новых уголовно-правовых запретов, определить эффективность правоприменения и способность довести уголовное дело до суда, доказуемость признаков соответствующего состава преступления. Согласно данным, представленным Судебным департаментом при Верховном Суде РФ, в 2018 г. по ст. ст. 274[1] УК РФ не было осуждено ни одного человека, в 2019 г. было осуждено 4 лица, в 2020 г. — 8, в 2021 г. — 15, в 2022 г. число осужденных составило 57 человек[4]. При этом показатель осуждений по сравнению с числом зарегистрированных преступлений снизился, что может указывать на наличие прикладных трудностей, связанных с пониманием содержания признаков неправомерного воздействия на объекты КИИ.

Нельзя не отметить, что особую актуальность вопросы уголовно-правовой охраны КИИ приобрели в период проведения специальной военной операции на Украине. В 2022 – 2023 гг. количество компьютерных атак на информационные ресурсы государственных и муниципальных органов власти кратно возросло. Зачастую указанные деяния совершаются в целях последующего размещения заведомо ложной информации, возбуждения паники среди населения, подпитки протестных реакций в обществе. С угрозами организованного деструктивного цифрового воздействия сталкиваются и крупные субъекты экономической деятельности.

---

[3] ФКУ «ГИАЦ МВД России» : официальный сайт. URL: www.мвд.рф (дата обращения: 04.04.2023).

[4] Официальный сайт Судебного департамента при Верховном Суде Российской Федерации : официальный сайт. URL: www.cdep.ru (дата обращения: 04.04.2023).

Серьезные игроки рынка стратегического управления цифровыми рисками отмечают существенный рост атак на российский оборонно-промышленный комплекс и объекты КИИ в 2022 – 2023 гг.[5].

В правоприменительной практике возникает множество вопросов относительно толкования признаков состава преступления, предусмотренного ст. 274[1] УК РФ. Отмечаются проблемы, связанные с отграничением неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, от смежных составов преступлений. К сожалению, в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 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"»[6] (далее — Постановление Пленума № 37/2022) данные проблемы не получили своего разрешения. В отечественной доктрине уголовного права либо не разработаны, либо являются остро дискуссионными многие вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. К тому же саму конструкцию ст. 274[1] УК РФ нельзя признать оптимальной во многих отношениях.

Изложенное позволяет заключить, что исследование вопросов законодательного определения и квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации является актуальной задачей для российской уголовно-правовой науки и правоприменительной практики. Указанные обстоятельства в совокупности обусловили выбор диссертантом темы научного исследования.

Степень научной разработанности темы исследования. На монографическом уровне проблемы уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации до настоящего времени не рассматривались.

Отдельные вопросы обозначенной темы освещались в научных статьях таких ученых, как И. Р. Бегишев, А. Г. Волеводз, Р. Р. Гайфутдинов, Ю. В. Грачева, Р.И. Дремлюга, К. Н. Евдокимов, М. А. Ефремова, Н. Ш. Козаев,

---

[5] *Никитина Т.* APT-группа Core Werewolf шпионит за российскими КИИ с помощью UltraVNC : URL : https://www.anti-malware.ru/news/2023-06-08-114534/41345 (дата обращения: 09.06.2023).

[6] Официальный сайт Верховного Суда РФ www.vsrf.ru (дата обращения: 04.04.2023).

Л. Ю. Ларина, В. Е. Новичков, Д. В. Пучков, И. Г. Пыхтин, А. Ю. Решетников, Е. А. Русскевич, О. М. Сафонов, А. В. Серебренникова, Э. Л. Сидоренко, Т. Л. Тропина, Ю. В. Трунцевский, З. И. Хисамова, И. Г. Чекунов, А. Ю. Чупрова и др.

Тем не менее приходится констатировать, что уровень теоретической разработки этой проблематики не соответствует ее сложности и значимости. В доктрине сохраняются разночтения в плане интерпретации признаков состава преступления, предусмотренного ст. 274^1 УК РФ; не получили должной проработки проблемы законодательного конструирования уголовно-правовой нормы об ответственности за неправомерное воздействие на КИИ; практически не исследованы в уголовно-правовом ракурсе и требуют научно обоснованного решения многие вопросы применения ст. 274^1 УК РФ.

Настоящее диссертационное исследование нацелено на восполнение отмеченных пробелов в научном знании, что дополнительно подчеркивает его актуальность.

Объектом исследования являются общественные отношения, возникающие в связи с установлением, дифференциацией и практической реализацией уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Предмет исследования составляют: неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации как преступление, предусмотренное ст. 274^1 УК РФ; признаки состава этого преступления; основания и критерии дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации; международно-правовые стандарты противодействия неправомерному воздействию на критическую информационную инфраструктуру; зарубежный опыт уголовно-правового противодействия преступлениям, связанным с неправомерным воздействием на критическую информационную инфраструктуру; проблемы квалификации преступлений, предусмотренных ст. 274^1 УК РФ.

Цель и задачи исследования. Цель работы заключается в теоретическом разрешении проблем, связанных с установлением, дифференциацией и реализацией уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, в разработке теоретических положений, которые могут быть положены в основу совершенствования конструкции ст. 274^1 УК РФ и практики ее применения.

Для достижения поставленной цели решены следующие исследовательские **задачи:**

- сформулированы предпосылки дифференциации уголовной ответственности за неправомерное воздействие на КИИ России;
- представлены результаты анализа международно-правовые стандарты противодействия посягательствам на КИИ;
- выявлены основные модели регламентации уголовной ответственности за посягательства на КИИ в зарубежных странах;
- установлено и уточнено содержание объективных уголовно-правовых признаков состава неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации;
- подвергнуто научному анализу и установлено содержание субъективных признаков преступления, предусмотренного ст. 274^1 УК РФ;
- представлены предложения по решению проблемных вопросов квалификации неправомерного воздействия на КИИ России;
- разработаны предложения по совершенствованию уголовно-правовой охраны КИИ.

Методология и методы исследования. Исследование проведено с использованием традиционного методологического инструментария. При изучении проблем уголовно-правового противодействия посягательствам на объекты КИИ применялись всеобщий философский метод познания, а также методы анализа, синтеза, дедукции, индукции, классификации, структурно-функциональный и др.

Формально-юридический и догматический методы использовались преимущественно при исследовании отечественного и зарубежного уголовного законодательства, материалов правоприменения.

Применение сравнительно-правового метода позволило установить основные модели уголовно-правовой охраны объектов КИИ в зарубежных странах, выявить положительный опыт, который может быть использован в УК РФ.

Значительное внимание уделено накоплению эмпирического материала, что потребовало проведения анкетирования, интервьюирования отдельных специалистов в IT-отрасли, анализа документов, печатных и электронных изданий.

Теоретической основой исследования послужили труды ученых-правоведов в различных отраслях права: гражданского, информационного,

международного, уголовного, уголовно-процессуального и др., в частности, работы по обозначенной теме Л. А. Букалеровой, Ю. В. Грачевой, М. А. Ефремовой, Н. Ш. Козаева, В. Н. Кудрявцева, Л. Л. Кругликова, А. В. Наумова, Н. И. Пикурова, Ю. Е. Пудовочкина, А. И. Рарога, Е. А. Русскевича, Т. Я. Хабриевой, А. И. Чучаева, В. Ф. Щепелькова и др.

Нормативную основу исследования составляют: Конституция Российской Федерации; международные правовые акты, посвященные противодействию преступности в сфере компьютерной информации, обеспечению международной информационной безопасности; федеральные законы Российской Федерации (в том числе кодифицированные), иные нормативные акты и официальные документы министерств и ведомств Российской Федерации, а также зарубежное законодательство.

Эмпирическая база исследования включает результаты анализа и обобщения:

- статистических данных Судебного департамента при Верховном Суде РФ, а также МВД России о применении ст. 274^1 УК РФ за период с 2018 по 2022 гг.;

- 215 решений судов о преступлениях в сфере компьютерной информации (ст. 272 – 274^2 УК РФ), в том числе 43 по делам о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК РФ), вынесенных в период с 2018 по 2022 гг.;

- данных проведенного в период с 2018 по 2022 гг. анкетирования 157 респондентов, среди которых доктора и кандидаты юридических наук, судьи, прокуроры и их помощники, адвокаты, следователи МВД России и Следственного комитета РФ, сотрудники оперативных подразделений органов внутренних дел, а также работники служб информационной безопасности организаций г. Москвы и Московской области по вопросам, относящимся к диссертационному исследованию;

- аналитических обзоров международных организаций, экспертно-аналитических отчетов российских и зарубежных компаний в IT-сфере;

- результаты анализа публикаций в СМИ в печатных и интернет-изданиях.

Научная новизна диссертации определяется содержанием ее положений и выводов, которые восполняют пробелы в части теоретического познания проблем уголовной ответственности за нарушение требований в области безопасности критической информационной инфраструктуры Российской Федерации, развивают уголовно-правовое учение о преступлениях в сфере компьютерной информации.

Новыми с научной точки зрения являются: теоретическое обоснование социально-правовой потребности в дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации; результаты исследования зарубежного законодательства об ответственности за преступления, связанные с неправомерным воздействием на КИИ; научно обоснованные решения сложных квалификационных проблем, возникающих при уголовно-правовой оценке неправомерного воздействия на КИИ России; частные правила квалификации этого преступления, которые предложено отразить в постановлении Пленума от 15 декабря 2022 г. № 37.

Критерию новизны отвечают так же предложения автора о содержании объективных и субъективных признаков состава преступления, предусмотренного ст. 274^1 УК РФ; авторская интерпретация отдельных конструктивных признаков, основанная на международных стандартах, позитивном законодательстве, специальных познаниях в области IT технологий; рекомендации по совершенствованию российского уголовного законодательства, базирующиеся, в том числе, на положительном зарубежном опыте.

Научную новизну диссертационного исследования подтверждают **основные положения, выносимые на защиту:**

1. Авторская аргументация идеи дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, реализованная законодателем путем выделения отдельной уголовно-правовой нормы. Такое решение соответствует современным вызовам и угрозам, возникающим на фоне процесса цифровизации жизнедеятельности. Выделение нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации позволило ликвидировать имевшийся дисбаланс в уголовном законе. Вместе с тем в технико-юридическом плане дифференциацию уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации трудно признать оптимальной. При конструировании ст. 274^1 УК РФ допущены серьезные просчеты, которые снижают эффективность уголовно-правовой охраны отношений, обеспечивающих информационную безопасность.

2. Разработана авторская классификация источников международного права, определяющих основы защиты объектов КИИ:

а) акты первого поколения, направленные на гармонизацию усилий и законодательств государств в сфере противодействия киберпреступности в целом;

б) международные документы второго поколения, принятые в целях разрешения отдельных вопросов эффективной защиты именно объектов критической информационной инфраструктуры.

Международное право, применимое на современном этапе к отношениям в сфере обеспечения безопасности КИИ, действует только между ограниченным кругом государств, для которых складывается соответствующая практика в силу регионального (локального) сотрудничества.

3. Доказано, что предметом преступления, предусмотренного ст. 274^1 УК РФ, является не компьютерная информация, содержащаяся в критической информационной инфраструктуре, а сам значимый объект критической информационной инфраструктуры (независимо от категории значимости), характеризующийся двумя критериями: *критерием значимости*, то есть особой социальной, политической, экономической, экологической или оборонной (для безопасности государства и правопорядка) важности (ст. 7 Федерального закона от 26 июля 2017 г. № 187-ФЗ) и *реестровым критерием*, связанным с включением объекта в реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26 июля 2017 г. № 187-ФЗ).

Для признания соответствующего объекта информационной инфраструктуры предметом преступления, предусмотренного ст. 274^1 УК РФ, необходимо наличие обоих указанных критериев.

4. Определено, что под вредом по смыслу ч. 2 ст. 274^1 УК РФ следует понимать:

а) нарушение функционирования объекта критической информационной инфраструктуры;

б) прекращение функционирования объекта критической информационной инфраструктуры;

в) нарушение функционирования сети электросвязи, используемой для организации взаимодействия таких объектов;

г) прекращение функционирования сети электросвязи, используемой для организации взаимодействия таких объектов;

д) нарушение безопасности обрабатываемой таким объектом информации.

5. Представлены предложения по квалификации неправомерного воздействия на КИИ:

1) при решении вопроса об обратной силе уголовного закона следует учитывать, что действия лица, направленные на вмешательство в функционирование программных или программно-аппаратных средств, которые

субъектом не были категорированы и, соответственно, не были включены Федеральной службой по техническому и экспортному контролю (ФСТЭК России) в реестр значимых объектов КИИ, не могут оцениваться в рамках ст. 274^1 УК РФ и требуют квалификации по ст. 272 УК РФ;

2) лицо, фактически выполняющее определенные профессиональные функции с объектами критической информационной инфраструктуры в отсутствие нормативно определенной обязанности соблюдать соответствующие правила доступа и эксплуатации, не может быть признано субъектом преступления, предусмотренного ч. 3 ст. 274^1 УК РФ;

3) вопрос о пределах вменения при соучастии в неправомерном воздействии на КИИ должен решаться с учетом объема вины. Заблуждение одного из соучастников относительно направленности совершаемого деяния на КИИ исключает возможность квалификации содеянного по ч. 1 или ч. 2 ст. 274^1 УК РФ. В зависимости от фактических обстоятельств содеянного действия такого лица могут быть квалифицированы по ст. 272 УК РФ и (или) ст. 273 УК РФ;

4) неправомерный доступ к КИИ, совершенный группой лиц по предварительному сговору (ч. 4 ст. 274^1 УК РФ), имеет место и тогда, когда один из соучастников осуществил проникновение в защищенную информационную систему, а другие в последующем совершили манипуляции с компьютерной информацией, что повлекло причинение вреда критической информационной инфраструктуре Российской Федерации;

5) если лицо имело намерение совершить компьютерную атаку на КИИ, но по ошибке причинило вред не категорированным объектам, юридическая оценка содеянного должна быть дана в соответствии с направленностью умысла виновного, то есть по ст. 274^1 УК РФ со ссылкой на ч. 3 ст. 30 УК РФ;

6. В целях повышения эффективности уголовно-правового противодействия посягательствам на КИИ, сформулированы предложения по совершенствованию:

6.1. *Российского уголовного законодательства*. В частности, предлагается: дополнить п. 8 ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и изложить его в новой редакции; изложить ст. 274^1 УК РФ в новой редакции; дополнить гл. 28 УК РФ новой нормой об установлении ответственности за нарушение требований в области безопасности критической информационной инфраструктуры Российской Федерации (проектируемая ст. 274^3 УК РФ); дополнить гл. 34 УК РФ специальной нормой об ответственности за планирование, подготовку, развязывание и ведение информационной войны;

6.2. *Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 г.* В ст. 3 указанного Соглашения предлагается включить пункт «в[1]» следующего содержания: «неправомерное воздействие на критическую информационную инфраструктуру, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, нарушение работы информационной (компьютерной) системы либо причинение иного существенного вреда»;

6.3. *Правоприменительной практики* по ст. 274[1] УК РФ путем изменения содержания постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 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"» (авторский вариант проекта постановления Пленума ВС РФ представлен в приложении А).

Теоретическая значимость исследования заключается в дальнейшем развитии отечественной теории уголовного права об ответственности за преступления в сфере компьютерной информации, и прежде всего об ответственности за посягательства на объекты критической информационной инфраструктуры. В работе представлены уточнения категориального аппарата, новые подходы к определению конструктивных признаков ст. 274[1] УК РФ, приведены авторские классификации отдельных явлений. Теоретической значимостью обладают также положения об ответственности за исследуемое преступление по законодательству зарубежных стран.

Практическая значимость работы. Отдельные положения диссертации могут быть полезны и напрямую использованы в самых разных областях, поскольку направлены, прежде всего, на упорядочение современного правоприменения и в этом отношении служат инструментом в решении конкретных практических задач сотрудников правоохранительных органов, адвокатов и судей. Некоторые выводы и рекомендации будут полезны для деятельности государственного регулятора в сфере критической информационной инфраструктуры — ФСТЭК России, а также могут быть использованы в образовательном процессе при изучении курсов уголовного права, информационного права, информационной безопасности и др. И наконец, в работе предложены готовые решения для осуществления законотворческой деятельности в исследуемой области. Также материалы диссертации могут быть

использованы в просветительской деятельности в области цифровой гигиены и информационной безопасности. Материалы исследования используются в учебном процессе НОУ ОВО «Российская академия адвокатуры и нотариата» и в работе Департамента государственной регистрации ведомственных нормативных правовых актов Министерства юстиции Российской Федерации.

Степень достоверности и апробация результатов исследования. Комплексно результаты исследования отражены в монографии «Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру». Отдельные наиболее значимые выводы были опубликованы в 1 монографии и 6 научных статьях: 4 — в изданиях, рекомендованных Высшей аттестационной комиссией при Минобрнауки России; 2 — в сборниках, подготовленных по результатам международных научно-практических конференций.

Кроме того, основные результаты проведенного исследования обсуждались на заседаниях кафедры адвокатуры и уголовно-правовых дисциплин Российской академии адвокатуры и нотариата и были предметом докладов и выступлений на различных научно-практических конференциях: XVIII Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (Москва, Московский государственный юридический университет имени О. Е. Кутафина (МГЮА), 21–22 января 2021 г.), I Всероссийской научно-практической конференции «Цифровые технологии в борьбе с преступностью: проблемы, состояние, тенденции (Долговские чтения) (Москва, Университет прокуратуры РФ, 27 января 2021 г.), Международной научно-практической конференции «Уголовная политика и культура противодействия преступности» (Краснодар, Краснодарский университет МВД России, 24 сентября 2021 г.), Всероссийской научно-практической конференции «Современные проблемы обеспечения защиты прав российских граждан и юридических лиц в условиях международных санкций» (Москва, Российская академия адвокатуры и нотариата, 6 декабря 2022 г.), II Всероссийской конференции «Уголовная политика в условиях цифровой трансформации» (Казань, Казанский филиал Российского государственного университета правосудия, 27 апреля 2023 г.) и др.

Структура диссертации обусловлена целями и задачами предлагаемого исследования и соответствует требованиям ГОСТ Р 7.0.11-2011. Работа состоит из введения, трех глав, объединяющих семь параграфов, заключения, библиографического списка и приложений.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы диссертационного исследования, определяются его цели и задачи, объект и предмет, характеризуются методологическая, нормативная, теоретическая и эмпирическая основы, рассматривается научная новизна, теоретическая и практическая значимость работы, сформулированы основные положения, выносимые на защиту, приводятся данные об апробации и внедрении полученных результатов.

Первая глава диссертации – «**Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: общетеоретические аспекты»** – состоит из трех параграфов. В первом из них – **«Социально-правовые предпосылки дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»** – рассматриваются социально-криминологические основания специального определения ответственности за посягательства на объекты критической информационной инфраструктуры Российской Федерации. Автор делает вывод, что реализованная законодателем дифференциация уголовной ответственности соответствует современным вызовам и угрозам, возникающим на фоне процесса цифровизации жизнедеятельности. Выделение нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации позволило ликвидировать имевшийся дисбаланс в уголовном законе, что позволяет оценить это законодательное решение положительно. Вместе с тем в исследовании обосновывается, что в технико-юридическом плане дифференциацию уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации нельзя признать оптимальной. При конструировании статьи 274^1 УК РФ допущены серьезные просчеты, которые снижают эффективность уголовно-правовой охраны отношений, обеспечивающих информационную безопасность.

Второй параграф первой главы диссертации посвящен анализу **международно-правовых стандартов в противодействии неправомерному воздействию на критическую информационную инфраструктуру.** Соискатель делает вывод, что система международных документов, в той или иной мере затрагивающих вопросы противодействия неправомерному воздействию на критическую информационную инфраструктуру к настоящему времени

представлена следующими элементами: международные документы первого поколения, направленные на гармонизацию усилий и законодательств государств в сфере противодействия киберпреступности в целом; международные документы второго поколения, принятые в целях разрешения отдельных вопросов эффективной защиты именно объектов критической информационной инфраструктуры. К отношениям в сфере обеспечения безопасности критической информационной инфраструктуры международное право действует только между ограниченным кругом государств, для которых складывается соответствующая практика в силу регионального (локального) сотрудничества.

По мнению диссертанта, Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий, как основной документ о противодействии цифровой преступности в регионе, требует доработки путем включения в статью 3 пункта «в[1]» в следующей редакции: «неправомерное воздействие на критическую информационную инфраструктуру, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, нарушение работы информационной (компьютерной) системы либо причинение иного существенного вреда».

Одновременно с этим предлагается дополнить статью 1 данного Соглашения понятием объекта информационно-коммуникационной инфраструктуры – совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, средств обеспечения функционирования такого объекта, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, а также персонала, который осуществляет их эксплуатацию.

Отвечающим современным угрозам является дальнейшее совершенствование отечественного уголовного законодательства в части установления ответственности за преступления против мира и безопасности человечества (глава 34 УК РФ). Автор обосновывает, что перспективным является дополнение соответствующей главы УК РФ специальной нормой об ответственности за планирование, подготовку, развязывание и ведение информационной войны, определение которой уже получило свое отражение в отдельных международных документах регионального уровня.

Третий параграф первой главы посвящен анализу **основных подходов к определению ответственности за преступления, связанные с неправомерным**

воздействием на критическую информационную инфраструктуру, в законодательстве зарубежных стран. По способу юридического закрепления уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру, соискатель действующие уголовные законодательства зарубежных государств разделяет на три группы: 1) страны, в которых обозначенный вопрос решается путем законодательной регламентации только общих положений об ответственности за преступления в сфере компьютерной информации (Беларусь, Буркина Фасо, Канада, Узбекистан); 2) страны, в которых совершение деяния в отношении критической информационной инфраструктуры выступает квалифицирующим признаком преступлений в сфере компьютерной информации (Австрия, Азербайджан, Германия, Италия, Казахстан, Латвия, Франция); 3) уголовные законодательства государств, включающие специальные нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру, формируют третью группу (Ботсвана, Великобритания, Замбия, Кения, Мальта, Нигерия, США, Уганда).

Проведенный анализ зарубежного законодательства позволил выявить практику криминализации нарушения требований в области обеспечения безопасности критической информационной инфраструктуры лицом, в силу выполняемой работы или занимаемой должности обязанным соблюдать эти правила. Такие составы преступлений могут быть совершены только специальными субъектами, включенными в специфическую группу общественных отношений, связанных с владением и (или) эксплуатацией объектов критической информационной инфраструктуры (Сингапур, Кения, ЮАР).

Вторая глава диссертации – «**Юридический анализ неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации**» – состоит из двух параграфов. Первый из них посвящен **уголовно-правовой характеристике объективных признаков неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.**

Соискатель делает вывод, что объектом преступления, предусмотренного ст. 274^1 УК РФ, являются общественные отношения, связанные с построением и развитием в Российской Федерации информационного общества, цифровой экономики и электронного правительства.

Предметом преступления, предусмотренного ст. 274[1] УК РФ, является не компьютерная информация, содержащаяся в критической информационной инфраструктуре, а сам значимый объект критической информационной инфраструктуры (независимо от категории значимости), характеризующийся двумя критериями: а) объективный критерий социальной, политической, экономической, экологической или оборонной (для безопасности государства и правопорядка) значимости (ст. 7 Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»); б) формальный критерий, связанный с включением объекта в реестр значимых объектов критической информационной инфраструктуры (ст. 8 Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»). Для признания соответствующего объекта информационной инфраструктуры предметом преступления, предусмотренного ст. 274[1] УК РФ, необходимо наличие двух указанных критериев.

Перечень отраслей, в которых могут быть выделены объекты критической информационной инфраструктуры, является искусственно ограниченным. Совершение компьютерных атак на автоматизированные системы управления в ряде других отраслей экономики, может вызвать не меньшие негативные последствия, чем на транспорте или в сфере связи. С учетом этого обосновывается, что п. 8 ст. 2 Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» необходимо дополнить, изложив в следующей редакции: «субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, строительства, транспорта, жилищно-коммунального хозяйства, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической, химической и пищевой промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей».

По ч. 1 ст. 274[1] УК РФ как использование вредоносной компьютерной программы (информации) нельзя оценивать действия лица, выражающиеся в ее хранении и изучении, а также в тестировании, направленном на установление особенностей ее функционирования и (или) на получение информации о возможном разработчике и т.п.

По смыслу ст. 274[1] УК РФ, под вредом следует понимать: а) нарушение функционирования объекта критической информационной инфраструктуры; б) прекращение функционирования объекта критической информационной инфраструктуры; в) нарушение функционирования сети электросвязи, используемой для организации взаимодействия таких объектов; г) прекращение функционирования сети электросвязи, используемой для организации взаимодействия таких объектов; д) нарушение безопасности обрабатываемой таким объектом информации.

Если нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, были нарушены двумя или более лицами, обладающими признаками субъекта преступления, предусмотренного ч.3 или ч.4 ст. 274[1] УК РФ, то содеянное каждым из них влечет уголовную ответственность по данной норме при условии, что допущенные ими нарушения специальных правил находились в причинной связи с наступившими последствиями.

В диссертации обосновывается, что ч. 5 ст. 274[1] УК РФ необходимо изложить в следующей редакции: «Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления».

Второй параграф второй главы диссертации раскрывает **уголовно-правовую характеристику субъективных признаков неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.**

Соискатель делает вывод, что подлинно научный ответ на вопрос о снижении возраста уголовной ответственности за преступления в сфере компьютерной информации в целом и неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, в частности, юридическая наука сможет дать только в том случае, когда будет

проведена комплексная (и думается, многолетняя) работа по изучению связей между движением современной «диджитализированной» преступности и развитием различных сторон общественной жизни, закономерностей отражения различных мер социального контроля и принуждения в общественном и индивидуальном сознании, а также деятельности судебно-следственных органов и системы исполнения наказания. Пока же этот опыт недостаточен, решение о снижении возраста уголовной ответственности за преступления в сфере компьютерной информации является преждевременным.

Если лицо фактически выполняет определенные профессиональные функции с объектами критической информационной инфраструктуры в отсутствие нормативно определенной обязанности соблюдать соответствующие правила доступа и эксплуатации, то оно не может быть признано субъектом преступления, предусмотренного ч. 3 ст. 274^1 УК РФ.

Толкование служебного положения лица как квалифицирующего признака неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации носит двойственный характер: а) применительно к ч. 1 и 2 ст. 274^1 УК РФ оно должно быть расширительным – в качестве такого лица может выступать любое лицо, обязанное в силу выполняемых ими профессиональных функций, соблюдать и (или) обеспечивать информационную безопасность объектов критической информационной инфраструктуры Российской Федерации; б) в отношении деяния, описанного ч. 3 ст. 274^1 УК РФ, оно является ограничительным – должностные лица, обладающие признаками, предусмотренными п. 1 примечания к ст. 285 УК РФ, государственные или муниципальные служащие, не являющиеся должностными лицами, а также иные лица, отвечающие требованиям, предусмотренным п. 1 примечания к ст. 201 УК РФ.

Если лицо, опираясь на объективные факторы, по ошибке атаковало объект критической информационной инфраструктуры Российской Федерации, квалифицировать содеянное по ст. 274^1 УК РФ нельзя. В данном случае квалификация содеянного должна осуществляться по общей норме об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ). При этом, учитывая, что доступ был осуществлен к объектам критической информационной инфраструктуры Российской Федерации, оценивать содеянное как повлекшее наступление тяжких последствий, то есть по ч. 4 ст. 272 УК РФ.

Третья глава диссертации – «**Вопросы совершенствования уголовного законодательства и проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации**» – состоит из двух параграфов.

В первом параграфе анализируются **проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации.** Соискатель делает вывод, что неправомерный доступ к критической информационной инфраструктуре, совершенный группой лиц по предварительному сговору (ч. 4 ст. 274^1 УК РФ), имеет место и в том случае, когда один из соучастников осуществил проникновение в защищенную информационную систему, а другие в последующем совершили манипуляции с компьютерной информацией, что повлекло причинение вреда критической информационной инфраструктуре Российской Федерации. Вопрос о пределах вменения при соучастии в неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации должен решаться с учетом объема вины. Заблуждение одного из соучастников относительно направленности совершаемого деяния на критическую информационную инфраструктуру Российской Федерации исключает возможность квалификации содеянного по ч. 1 или 2 ст. 274^1 УК РФ. В зависимости от фактических обстоятельств содеянного действия такого лица могут быть квалифицированы по ст. 272 УК РФ и (или) ст. 273 УК РФ.

Если лицо намеревалось совершить компьютерную атаку на критическую информационную инфраструктуру Российской Федерации, но по ошибке причинило вред не категорированным объектам, юридическая оценка содеянного должна быть дана в соответствии с направленностью умысла виновного, то есть по ст. 274^1 со ссылкой на ч. 3 ст. 30 УК РФ. Если неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации осуществлялось под непосредственным контролем правоохранительных органов (в рамках проверочной закупки, оперативного эксперимента и т.д.) содеянное необходимо квалифицировать как неоконченное преступление.

В целях упорядочения формирующейся правоприменительной практики по ст. 274^1 УК РФ предлагается внести дополнения в постановление Пленума Верховного Суда Российской Федерации № 37 от 15 декабря 2022 г. «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"» (проект постановления приведен в приложении А, с. 181–183 диссертации).

Во втором параграфе третьей главы диссертации исследуются **основные направления совершенствования уголовного законодательства об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.**

Автор обусловливает настоятельную необходимость законодательной коррекции уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Предлагается следующая редакция нормы, предусмотренной ст. 274^1 УК РФ, а также проектируемая ст. 274^3 УК РФ:

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

1. 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, –

наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

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, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации, –

наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением

свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, –

наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

4. Деяния, предусмотренные частью первой, второй или третьей настоящей статьи, совершенные:

а) в отношении объекта критической информационной инфраструктуры второй категории;

б) группой лиц по предварительному сговору или организованной группой;

в) лицом с использованием своего служебного положения, –

наказываются лишением свободы на срок от трех до восьми лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

5. Деяния, предусмотренные частью первой, второй, третьей или четвертой настоящей статьи, если они совершены в отношении объекта критической информационной инфраструктуры первой категории либо повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового.

Статья 274[3]. Нарушение требований в области безопасности критической информационной инфраструктуры Российской Федерации

1. Неисполнение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации лицом, в силу выполняемой им работы или занимаемой должности обязанным соблюдать эти правила, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, –

наказывается принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

2. Деяние, предусмотренное частью первой настоящей статьи, если оно совершено в отношении объекта критической информационной инфраструктуры второй категории, –

наказывается лишением свободы на срок от трех до шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового

3. Деяние, предусмотренное частью первой настоящей статьи, если оно совершено в отношении объекта критической информационной инфраструктуры первой категории либо повлекло тяжкие последствия или создало угрозу их наступления, –

наказывается лишением свободы на срок от пяти до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до пяти лет или без такового».

В **заключении** подведены итоги проведенного исследования, сформулированы его основные положения и выводы.

В **библиографии** в систематизированном виде представлены источники, использованные при написании диссертации.

В **приложениях** представлен авторский проект постановления Пленума Верховного Суда РФ и в концентрированном виде приведены сведения о проведенном социологическом исследовании.

Список научных публикаций, в которых изложены основные научные результаты диссертации

I. Монография:

1. Малыгин, И. И. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру: монография / И. И. Малыгин. – М.: ИНФРА-М, 2023. – 164 с. (10,25 п.л.).

II. В рецензируемых научных изданиях, рекомендованных Высшей аттестационной комиссией при Министерстве науки и высшего образования Российской Федерации

2. Малыгин, И. И. Актуальные проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / И. И. Малыгин // Известия Юго-Западного государственного университета. Серия История и право. – 2023. – Т. 13. № 2. – С. 165-176. (0,5 п.л.).

3. Малыгин, И. И. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру по законодательству Южной Кореи, Бангладеш и Филиппин / И.И. Малыгин // Закон и право. – 2023. – № 5. – С. 226 – 228. (0,4 п.л.).

4. Малыгин, И. И. О совершенствовании уголовного законодательства об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации / И. И. Малыгин // Вестник Российской правовой академии. – 2021. – № 3. – С. 118-122. (0,4 п.л.).

III. В иных научных изданиях:

5. Малыгин, И. И. Социально-правовые предпосылки дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации / И. И. Малыгин // Уголовная политика и культура противодействия преступности: материалы Международной научно-практической конференции, Краснодарский университет МВД России (Краснодар, 24 сентября 2021 г.). – Краснодар: Краснодарский университет МВД России, 2021. – С. 271 – 276 (0,4 п.л.).

6. Малыгин, И.И. Уголовно-правовая характеристика субъекта неправомерного воздействия на критическую информационную инфраструктуру / И. И. Малыгин // Право. Адвокатура. Нотариат. Материалы Международных чтений. 19 апреля 2023 года. Под редакцией доктора юридических наук, профессора Р.В. Шагиевой и кандидата юридических наук, доцента Н.Н. Косаренко. – М.: Русайнс, 2023. – С. 249 – 254 (0,4 п.л.).