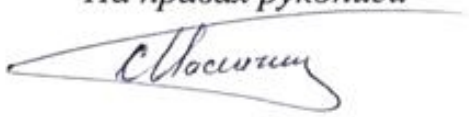
Негосударственное образовательное учреждение организация высшего образования «Российская академия адвокатуры и нотариата»

На правах рукописи



Малыгин Иван Игоревич

УГОЛОВНО-ПРАВОВОЕ ПРОТИВОДЕЙСТВИЕ НЕПРАВОМЕРНОМУ ВОЗДЕЙСТВИЮ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ

Специальность 5.1.4 — Уголовно-правовые науки

Диссертация
на соискание ученой степени
кандидата юридических наук

Научный руководитель:
доктор юридических наук, профессор
Букалерова Людмила Александровна

Москва — 2023

Оглавление

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].

---

[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.

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 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 %)[1]. 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[2]. 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

---

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

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

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.

Серьезные игроки рынка стратегического управления цифровыми рисками отмечают существенный рост атак на российский оборонно-промышленный комплекс и объекты КИИ в 2022 – 2023 гг.[1].

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"»[2] (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

---

[1] *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).

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

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, 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.), Международных научных чтениях «Право. Адвокатура. Нотариат» (Москва, Российская академия адвокатуры и нотариата, 19 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.

Глава 1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: общетеоретические аспекты

Познание объекта настоящего исследования невозможно без предварительного погружения в комплекс вопросов о социально-правовых предпосылках дифференциации ответственности за неправомерное воздействие на КИИ. На этом этапе необходимо осмыслить логику принятого решения, его социально-политический смысл и правовой эффект, которые учитывал и к которым стремился законодатель.

Неразрывно с этим следует разобраться с международно-правовыми стандартами противодействия посягательствам на информационные объекты особого (критического) значения. Какими бы ни были суждения о значимости международного права в современном мироустройстве, все-таки глобализм компьютерных преступлений заставляет смотреть на эту проблему как на проблему обеспечения не только национальной, но и международной безопасности.

И наконец, значимым блоком настоящего исследования видится проведение компаративистского исследования уголовного законодательства зарубежных стран. Именно по этой причине зарубежный аспект включен в название работы. Российская Федерация не является пионером в области уголовно-правовой охраны критической информационной инфраструктуры. По ряду объективных причин мы во многом «догоняем» другие страны, которые гораздо раньше обратили внимание на эту проблему и уже накопили серьезный опыт. Цель сравнительно-правового анализа состоит в выявлении общих закономерностей в криминализации и пенализации посягательств на критическую информационную инфраструктуру.

Все это в совокупности, на наш взгляд, выступает теми обязательными пролегоменами, которые необходимы для четкого понимания и оценки

сложившегося состояния, а также научного обоснования предложений по совершенствованию конструкции и (или) применения ст. 274[1] УК РФ.

§ 1. Социально-правовые предпосылки дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Принципиально важной и отправной задачей настоящего исследования является выявление и анализ тех социально-правовых предпосылок, которые обусловили принятие законодателем решения о дифференциации уголовной ответственности за посягательства на объекты информационной инфраструктуры повышенного (особого) значения. В отечественной теории уголовного права ученые уже обращались к данной проблематике. В целом специалисты сходятся во мнении, что динамика преступлений в сфере компьютерной информации подтверждает необходимость и своевременность «имплементации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации и усиления противодействия данному виду общественно опасного деяния»[1].

Полагаем, что применительно к ст. 274[1] УК РФ необходимо говорить именно о дифференциации ответственности, а не о криминализации, поскольку, как и большинство отечественных специалистов[2], мы разделяем позицию, согласно которой описанные в ст. 274[1] УК РФ деяния являлись преступными и

---

[1] *Новичков В. Е., Пыхтин И. Г.* Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Психопедагогика в правоохранительных органах. 2018. № 2 (73). С. 25.

[2] См., например: *Дремлюга Р. И., Зотов С. С., Павлинская В. Ю.* Критическая инфраструктура как предмет преступного посягательства // Азиатско-тихоокеанский регион: экономика, политика, право. 2019. № 2. С. 134; *Решетников А. Ю., Русскевич Е. А.* Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК России) // Законы России: опыт: анализ, практика. 2018. № 2 (66). С. 51–55. и др.

до принятия Федерального закона от 26 июля 2017 г. № 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"» (далее — Закон № 194-ФЗ/2017). Нельзя не отметить, что такой подход был изначально выражен и в пояснительной записке Правительства РФ к проекту указанного закона: «Статья 14 проекта федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации" наряду с дисциплинарной, гражданско-правовой и административной ответственностью предусматривает уголовную ответственность граждан Российской Федерации, иностранных граждан и лиц без гражданства за нарушение законодательства о безопасности критической информационной инфраструктуры Российской Федерации. В настоящее время ответственность за такие деяния может наступать на основаниях, предусмотренных статьями 272–274 Уголовного кодекса Российской Федерации. Вместе с тем, учитывая необходимость повышенной уголовно-правовой защиты безопасности критической информационной инфраструктуры Российской Федерации целесообразно выделение составов посягательств на критическую информационную инфраструктуру Российской Федерации в отдельную статью»[1].

Таким образом, в июле 2017 г., используя средства Особенной части УК РФ, законодатель осуществил целевую «настройку» механизма уголовно-правовой охраны с целью обеспечения реализации Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее — Закон о безопасности КИИ России).

Вместе с тем такое решение не может не вызывать вопросов, требующих своего осмысления и проработки. С уголовно-политической точки зрения в

[1] Пояснительная записка Правительства Рос. Федерации к проекту федерального закона № 47591-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Система обеспечения законодательной деятельности : сайт. URL: www.sozd.duma.gov.ru (дата обращения: 20.10.2021).

пояснительной записке не было представлено веских оснований в пользу ужесточения ответственности за неправомерное воздействие на критическую информационную инфраструктуру. Как справедливо резюмирует Л. Ю. Ларина, в законопроекте лишь констатируется необходимость повышенной уголовно-правовой защиты безопасности КИИ. При этом не приводится каких-либо аргументов в подтверждение этого вывода[1].

М. А. Ефремова полагает, что законодатель ошибся с определением места данной статьи в Особенной части УК РФ. По мнению автора, ее следовало бы включить в гл. 24 УК РФ «Преступления против общественной безопасности», так как по сути ст. 274[1] УК РФ представляет собой криминализацию кибертерроризма[2].

Здесь сразу надо подчеркнуть, что имманентность создания угрозы для неограниченного круга лиц все же выступает довольно слабым аргументом в пользу того, чтобы говорить об ошибочности определения видового объекта. Безусловно, общественная безопасность в той или иной форме затрагивается посягательством, предусмотренным исследуемой нормой, но ведь вопрос должен быть поставлен о том, является ли это непосредственной и главной мишенью. Полагаем, что не является. Равно как и применение к неправомерному воздействию на объекты КИИ такого термина, как «кибертерроризм», выступает лишь навешиванием эффектного ярлыка на деяние, которое довольно часто по своему содержанию не обладает известным масштабом. Согласившись с этим, мы будем принуждены именовать кибертеррористами работников организаций связи, которые торгуют данными из служебной категорированной системы, — наиболее распространенная практика по ст. 274[1] УК РФ в современных условиях.

Предсказуемо не нашло своего объяснения и построение санкций в проектируемой ст. 274[1] УК РФ. М. А. Простосердов небезосновательно

---

[1] См.: *Ларина Л. Ю.* Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру России // Актуальные вопросы борьбы с преступлениями. 2017. № 3. С. 23.

[2] См.: *Ефремова М. А.* Уголовно-правовые средства противодействия кибертерроризму // Уголовное право: стратегия развития в XXI веке : материалы XVII Междунар. науч.-практ. конф. М., 2020. С. 152.

отмечает по данному поводу, что при добавлении новых норм в Особенную часть УК РФ либо при внесении изменений в старые законодатель зачастую не уделяет особого внимания вопросу построения санкций таких норм, их согласования с диспозициями, а также с друг другом[1].

В юридико-техническом смысле возник вопрос о целесообразности самого введения специальной нормы, когда повышенную ответственность за подобные деяния можно и логично было бы установить посредством совершенствования системы квалифицирующих и особо квалифицирующих признаков ст.ст. 272–274 УК РФ[2].

В результате у специалистов сложилось представление, что изменения в УК РФ имели конъюнктурный характер, были подготовлены второпях, без должной проработки поставленной задачи, а само появление отдельной ст. 274[1] УК РФ ничего, кроме путаницы, конкуренции норм и квалификационных ошибок, не принесет. В этой связи представляется уместным привести умозаключение А. Н. Тарбагаева о том, что «вновь созданная юридическая норма должна отражать и закреплять реальные общественные отношения, соответствуя истинным потребностям общества, а не служить инструментом для удовлетворения сиюминутных интересов, создавая тем самым лишь видимость своей объективной необходимости»[3].

Можно ли из вышесказанного заключить, что выделение нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации является необоснованным? Полагаем, что ответ на данный вопрос все-таки должен быть отрицательным. Само по себе решение законодателя об установлении в специальной норме повышенной ответственности за такие действия

---

[1] См.: *Простосердов М. А.* Система санкций Особенной части Уголовного кодекса Российской Федерации: анализ, проблемы, пути решений : монография. М. : РГУП, 2020. С. 7.

[2] См. об этом: *Комаров А. А*. Отдельное мнение относительно законопроекта «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» // Вестник Северо-Кавказского гуманитарного института. 2017. № 3.

[3] *Тарбагаев А. Н*. Ответственность в уголовном праве // Правоведение. 1994. № 3. С. 102.

соответствует всем необходимым основаниям и условиям дифференциации уголовной ответственности.

Российская уголовно-правовая литература насчитывает не одно серьезное исследование о содержании, видах, средства, а также критериях дифференциации уголовной ответственности[1]. В рамках настоящей работы нет необходимости обстоятельно рассматривать каждый из этих общетеоретических вопросов. Решая задачу выделения и познания социально-правовых предпосылок дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации в УК РФ, остановимся лишь на релевантных пунктах данного учения.

Согласно представлениям Т. А. Лесниевски-Костаревой дифференциация ответственности есть «градация, разделение, расслоение ответственности в уголовном законе, в результате которой законодателем устанавливаются различные уголовно-правовые последствия в зависимости от типовой степени общественной опасности преступления и личности виновного»[2].

Несколько иначе понимает дифференциацию уголовной ответственности А. В. Васильевский: «изменение предусмотренного законом вида, размера и характера меры ответственности в зависимости от изменения общественной опасности деяния и лица, его совершившего, а также с учетом принципа гуманизма и других важных обстоятельств»[3].

Нетрудно заметить, что авторы раскрывают определение дифференциации уголовной ответственности преимущественно в непосредственной связи с материальным признаком преступления — общественной опасностью деяния.

---

[1] См.: *Васильевский А. В*. Дифференциация уголовной ответственности и наказания в Общей части уголовного права : дис. … канд. юрид. наук : 12.00.08. Ярославль, 2000; *Грибов А. С.* Дифференциация ответственности за экономические преступления в России, ФРГ и США: сравнительно-правовое исследование: автореф. дис. … канд. юрид. наук : 12.00.08. Ярославль, 2011; *Лесниевски-Костарева Т. А*. Дифференциация уголовной ответственности: теория и законодательная практика. М., 1998; *Рогова Е. В*. Учение о дифференциации уголовной ответственности : дис. … д-ра юрид. наук : 12.00.08. М., 2014 и др.

[2] *Лесниевски-Костарева Т. А*. Дифференциация уголовной ответственности: теория и законодательная практика. М., 1998. С. 52.

[3] *Васильевский А. В*. Дифференциация уголовной ответственности и наказания в Общей части уголовного права : дис. … канд. юрид. наук : 12.00.08. Ярославль, 2000. С. 4.

Как справедливо писал А. Э. Жалинский, «в основе практически любого решения в сфере уголовного правотворчества лежит оценка общественной опасности запрещаемого поведения, как деяния в целом, так и способов и обстоятельств его совершения»[1].

Е. В. Рогова также развивает идею, что общественная опасность (ее характер и степень) является определяющим критерием дифференциации уголовной ответственности[2].

В аспекте существования в уголовном законе специальных норм метко по этому поводу высказывается А. В. Архипов: «…специальная норма за совершение запрещенных ею деяний должна устанавливать уголовную ответственность, отличную от общей нормы. В противном случае выделение специальной нормы из общей становится просто бессмысленным»[3].

В свою очередь Е. А. Русскевич не без оснований дополняет: «…почти аксиоматичное представление о том, что дифференциация уголовной ответственности — это всегда проблема "подвижности" общественной опасности деяния, приобретает дискуссионный характер. В современных условиях дифференциация уголовной ответственности может иметь и другие — уголовно-политические, формально-юридические, а иногда и сугубо утилитарные (обусловленные обеспечением эффективности правоприменения) основания»[4].

Полагаем, что здесь можно согласиться как с мнением А. В. Архипова, так и поддержать позицию Е. А. Русскевича. Анализ последних изменений отечественного уголовного законодательства наглядно демонстрирует тот тезис,

---

[1] *Жалинский А. Э.* Оценка общественной опасности деяния в процессе уголовного правотворчества // Уголовное право: стратегия развития в XXI веке : Материалы 6-й междунар. науч.-практ. конф. (Москва, 29–30 января 2009 г.) М., 2009. С. 48.

[2] *Рогова Е. В.* Учение о дифференциации уголовной ответственности : дис. … д-ра юрид. наук : 12.00.08. М., 2014. С. 170.

[3] *Архипов В. П.* К вопросу о необходимости специальной нормы, предусматривающей уголовную ответственность за мошенничество при получении выплат // Вестник Томского государственного университета. 2013. № 377. С. 96.

[4] *Русскевич Е. А.* Уголовное право и «цифровая преступность»: проблемы и решения. М., 2019. С. 62.

что появление специальных норм не всегда может быть обусловлено желанием законодателя изменить подход к пенализации конкретного деяния.

Здесь как нельзя кстати можно привести высказывание В. Н. Кудрявцева: «…общая, абстрактная норма значительно удобнее для квалифицированного юриста. Но ведь уголовные законы создаются не только для юристов. Они имеют воспитательное и предупредительное значение. Простой и понятный текст закона, устанавливающего ответственность за конкретные действия, смысл которых ясен для любого гражданина, имеет важное профилактическое значение. Поэтому наряду с общими нормами, которые уже имеются в законодательстве, в некоторых случаях оправдано появление новых законов, подчеркивающих общественную опасность тех или иных форм поведения…»[1].

Таким образом, можно сделать вывод, что появление ст. 274[1] УК РФ было обусловлено сразу несколькими факторами. Во-первых, действия по неправомерному воздействию на объекты информационной инфраструктуры повышенной (особой) важности объективно обладают более высоким уровнем общественной опасности, поскольку представляют непосредственную угрозу не только отношениям по обеспечению информационной безопасности, но и в зависимости от особенностей деяния могут быть направлены против жизни и здоровья граждан, общественной безопасности, государственной власти и т. д.

Нанесение ущерба критической информационной инфраструктуре может привести к катастрофическим последствиям, а, учитывая, что она является связующим звеном между другими секторами национальной инфраструктуры, неизбежно нанесет ущерб и этим секторам. Переход информационных и коммуникационных технологий на систему цифровых сигналов упростил и частично автоматизировал управление процессами, но, в то же время, сделал их более уязвимыми перед компьютерными атаками. Вредоносная программа, направленная на внесение изменений в бинарный код программы способна вывести из строя любое оборудование, работающее с использованием бинарного кода. Компьютерная атака способна полностью парализовать критическую

[1] *Кудрявцев В. Н.* Общая теория квалификации преступлений. М., 1972. С. 248–249.

информационную инфраструктуру государства и вызвать социальную, финансовую и экологическую катастрофу[1].

Атаки на объекты критической информационной инфраструктуры любого государства всегда сопровождаются общественным резонансом и, как следствие, повышенным вниманием со стороны мирового сообщества. Учитывая те исключительные последствия, которые наступают или могут наступить вследствие неправомерного воздействия на них, само по себе это удивления не вызывает. Приведем несколько наиболее масштабных компьютерных инцидентов, связанных с атаками на объекты критической информационной инфраструктуры.

25 января 2003 г. для атаки на корпоративную сеть атомной электростанции в США была использована компьютерная программа «Slammer». Аналогичный инцидент повторился в декабре 2014 г. в Южной Корее. Требования злоумышленников не имели корыстного содержания и были связаны с деятельностью реакторов.

В декабре 2014 г. Федеральное управление по информационной безопасности Германии (BSI) опубликовало отчет, в котором анализировался случай кибератаки на информационную инфраструктуру одного из металлургических заводов страны. Злоумышленники использовали целенаправленный фишинг и смогли получить доступ к офисной и промышленной сетям предприятия. После заражения промышленного сегмента, начались «контролируемые» сбои на одной из доменных печей завода, в результате чего предприятию был нанесен значительный ущерб[2].

23 декабря 2015 г. в г. Ивано-Франковске (Украина) вдруг выключился свет: из строя одновременно вышли 30 подстанций, оставив без электричества сразу

---

[1] Пояснительная записка Правительства Рос. Федерации к проекту федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Система обеспечения законодательной деятельности : сайт. URL: www.sozd.duma.gov.ru (дата обращения: 15.11.2022).

[2] Bericht zur Lage der IT-Sicherheit in Deutschland 2014 [Электронный ресурс]. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf (дата обращения: 15.04.2022).

около 230 тыс. человек. Непосредственно перед отключением операторы подстанций могли наблюдать абсолютно мистические события: курсор мыши вдруг сам пополз по экрану, дополз до программы, контролирующей реле, активировал ее и разомкнул цепь, выключив подстанцию. А потом еще одну. И когда оператор компании «Прикарпатьеоблэнерго», очнувшись, попытался это остановить, его просто выкинуло из системы. Такие же события, но в меньших масштабах, происходили еще в двух компаниях, отвечавших за электроснабжение, — «Киевоблэнерго» и «Черновцыоблэнерго». В некоторых частях Ивано-Франковской области электроснабжение удалось восстановить только через 6 часов[1].

27 апреля 2016 г. в Германии компьютеры энергетической компании RWE оказались заражены вирусами «W32.Ramnit» и «Conficker»[2].

В марте 2019 г. в Венесуэле произошли два случая массового отключения электричества. Первая авария, которая случилась 7 марта на крупнейшей в стране ГЭС «Эль-Гури», привела к самому масштабному блэкауту в истории страны: 20 из 23 штатов были обесточены. 25 марта стало известно о массовых отключениях также из-за аварии на этой ГЭС, в результате без электричества остался по меньшей мере 21 из 23 штатов страны[3].

В настоящее время данный список компьютерных инцидентов с объектами критической информационной инфраструктуры можно продолжать довольно долго. Проблема уже давно перестала восприниматься как гипотетическая угроза и воспринимается рядом государств, в том числе и Россией, как компонент внешней безопасности и обороноспособности.

Появление ст. 274[1] УК РФ с уголовно-политической точки зрения направлено на обеспечение исполнения системообразующего законодательного

---

[1] 10 самых впечатляющих кибератак в истории [Электронный ресурс]. URL: https://3dnews.ru/1009634/10-samih-vpechatlyayushchih-kiberatak-v-istorii (дата обращения: 15.04.2022).

[2] Кибератаки на ядерные объекты: история вопроса // Газета «Коммерсантъ» : электронная версия. URL: https://www.kommersant.ru/doc/3196397 (дата обращения: 10.04.2022).

[3] Власти Венесуэлы установили причастных к атакам на энергосистему [Электронный ресурс] // РИА Новости. URL: https://ria.ru/20190423/1552985631.html (дата обращения: 15.04.2022).

акта, устанавливающего порядок отношений в сфере обеспечения безопасности критической информационной инфраструктуры в Российской Федерации.

Принятие столь значимого закона, который фактически затрагивает вопросы общественной и государственной безопасности, просто не могло не обернуться коррекцией механизма уголовно-правовой охраны. Иными словами, выделение ст. 274[1] УК РФ, конечно же, служит цели ужесточения наказания за деяния, обладающие качественно более высокой степенью общественной опасности в сравнении с преступлениями, предусмотренными ст.ст. 272–274 УК РФ. Однако само ее появление вступает в противоречие с юридической техникой отечественного уголовного закона, удовлетворяя при этом стремление законодателя придать задаче эффективного противодействия компьютерным атакам, способным парализовать критическую информационную инфраструктуру государства и вызвать социальную, финансовую и экологическую катастрофу, совершенно новый уровень внимания и фокус ответственности.

По мнению Л. Ю. Лариной, решение законодателя о введении отдельной нормы является ошибочным и неудачным[1]. Позволим себе не согласиться с автором. Введение ст. 274[1] УК РФ позволило ликвидировать дисбаланс в уголовном законе, о котором давно говорили ученые.

Еще до принятия Закона о безопасности КИИ России и введения его в действие А. В. Коротков и Е. С. Зиновьева в своей работе отмечали, что «критически важная инфраструктура имеет ключевое значение для общественного порядка, экономической стабильности и национальной безопасности государств… Защита критической инфраструктуры затрагивает вопросы национальной безопасности, и потому входит в компетенцию государства…»[2].

---

[1] *Ларина Л. Ю.* Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру России // Актуальные вопросы борьбы с преступлениями. 2017. № 3. С. 24.

[2] *Коротков А. В., Зиновьева Е. С.* Безопасность критических информационных инфраструктур в международном уголовном праве // Вестник МГИМО-Университета. 2011. № 4 (19). С. 156.

В этом же ключе А. В. Духвалов развивал идею об использовании информационных технологий повышенного значения для достижения политико-экономических целей: «…под такой киберприцел попал не только интернет-банкинг, но и электронная инфраструктура государственных органов, промышленных и военных объектов…»[1].

К. Н. Евдокимов предлагал пойти по пути дополнения ст.ст. 272–274 УК РФ указанием на совершение деяния: «с целью …воспрепятствования нормальной деятельности средств массовой информации, органов государственной власти и местного самоуправления, государственных и муниципальных учреждений, предприятий»[2].

Законодатель принял решение о выделении специальной нормы и тем самым обеспечил успешное решение сразу нескольких прикладных задач:

1) решен вопрос, связанный с подследственностью, — в отличие от остальных компьютерных преступлений, по делам о преступлении, предусмотренном ст. 274[1] УК РФ, предварительное расследование осуществляется следователями органов Федеральной службы безопасности;

2) созданы предпосылки для индивидуального статистического учета;

3) достигнут максимально возможный предупредительный эффект, вытекающий из самого факта изменения уголовного закона;

4) обеспечена возможность дифференциации уголовной ответственности за само неправомерное воздействие на объекты КИИ.

Полагаем, что указанные обстоятельства предельно четко выявляют логику принятия решения законодателем.

Обоснованность проведенной отечественным законодателем дифференциации подтверждается и зарубежным опытом. Обстоятельно данный вопрос будет освещен в § 3данной главы.

---

[1] *Духвалов А. П.* «Лаборатория Касперского» создает свою операционную систему // Право и кибербезопасность. 2012. № 1. С. 41–47.

[2] *Евдокимов К. Н.* Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты : монография. Иркутск, 2016. С. 84.

Завершая анализ социально-правовых предпосылок дифференциации уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации в УК РФ, следует отметить, что с момента появления ст. 274[1] УК РФ прошло не так уж много времени, но уже сегодня практика применения уголовно-правовой нормы позволяет говорить о ее востребованности. Согласно данным Судебного департамента при Верховном Суде РФ в 2018 г. за совершение преступления, предусмотренного ст. 274[1] УК РФ, не было осуждено ни одного человека, однако уже в 2019 г. осуждены 4 человека, в 2020 г. этот показатель увеличился в два раза до 8 человек, в 2021 еще в два раза (15 осужденных), в 2022 г. прирост составил 280 % по отношению к показателю предыдущего года – всего в 2022 г. было осуждено 57 человек[1].

В подтверждение изложенному можно привести приговор Первомайского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-376/2019. О., Л.А и Л.С. были осуждены по ч. 4 ст. 274[1] УК РФ. Как следует из приговора суда, злоумышленники, «используя компьютерную программу, получили удаленный доступ к ЭВМ АО «Восточная верфь», после чего осуществили неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, путем ее блокирования и модификации, что повлекло причинение вреда критической информационной инфраструктуре АО «Восточная верфь», а также причинение имущественного вреда указанной организации на сумму 655 034,52 руб.»[2].

Более того, на возрастающую востребованность у правоприменителей ст. 274[1] УК РФ указывают и ранее приведенные статистические данные МВД России, которые также свидетельствуют о расширении географии ее применения. Так, если в 2018 г. было зарегистрировано лишь одно преступление (Камчатский край), в 2019 г. — 4 (Амурская область – 1, Волгоградская область – 1,

---

[1] Официальный сайт Судебного департамента при Верховном Суде Российской Федерации: www.cdep.ru (дата обращения: 10.03.2023).

[2] Судебные и нормативные акты РФ : сайт. URL: www.sudact.ru (дата обращения: 20.01.2021).

Приморский край – 2), то в 2020 г. таких преступлений было зарегистрировано уже 22 (Амурская область – 1, Волгоградская область – 9, Ивановская область – 1, Кемеровская область – 1, г. Москва – 1, Мурманская область – 1, Пермский край – 1, Приморский край – 3, Республика Северная Осетия–Алания – 1, Республика Татарстан – 1, Республика Хакасия – 1, Тверская область – 1), в 2021 г — 159, а в 2022 г. их число увеличилось до 519[1].

Признавая обоснованность проведенной законодателем дифференциации, заметим, что в технико-юридическом плане ее нормативное воплощение нельзя признать оптимальным. При конструировании ст. 274[1] УК РФ допущены серьезные просчеты, которые снижают эффективность уголовно-правового противодействия деяниям, связанным с неправомерным воздействием на критическую информационную инфраструктуру Российской Федерации.

В теории уголовного права на это уже было обращено пристальное внимание. Так, например, А. Ю. Решетников и Е. А. Русскевич указывают на то, что «Федеральный закон от 26.07.2017 г. № 187-ФЗ предполагает категорирование всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка. При этом действующая редакция ст. 274[1] УК РФ не учитывает данное деление. В результате уголовно-правовая новелла не позволяет должным образом оценить различия в объеме и значимости социальных последствий криминальных посягательств на объекты критической инфраструктуры»[2].

Исследование вопроса о социально-правовых предпосылках дифференциации уголовной ответственности за неправомерное воздействие на КИИ позволяет сделать следующие выводы.

---

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

[2] *Решетников А. Ю., Русскевич Е. А.* Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК России) // Законы России: опыт: анализ, практика. 2018. № 2 (66). С. 55.

1. Реализованная законодателем дифференциация уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации соответствует современным вызовам и угрозам, возникающим на фоне процесса цифровизации жизнедеятельности.

2. Выделение специальной 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. Законодатель тем самым обеспечил успешное решение сразу нескольких прикладных задач:

1) решен вопрос, связанный с подследственностью — по делам о преступлении, предусмотренном ст. 274^1 УК РФ, предварительное расследование осуществляется следователями органов ФСБ России (в отличие от остальных компьютерных преступлений);

2) созданы предпосылки для индивидуального статистического учета;

3) достигнут максимально возможный предупредительный эффект, вытекающий из самого факта изменения уголовного закона;

4) обеспечена возможность дифференциации уголовной ответственности за само неправомерное воздействие на объекты КИИ.

3. В технико-юридическом плане дифференциацию уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации нельзя признать оптимальной. При конструировании ст. 274^1 УК РФ допущены серьезные просчеты, которые снижают эффективность уголовно-правовой охраны отношений, обеспечивающих информационную безопасность.

§ 2. Международно-правовые стандарты противодействия неправомерному воздействию на критическую информационную инфраструктуру

Рассмотрение вопросов международно-правового сотрудничества в целях обеспечения безопасности КИИ обладает совершенно особым теоретическим и практическим значением. Транснациональный характер подобных преступлений, когда компьютерная атака на социально значимые объекты государства может быть совершена из любой части нашей планеты, заставляет совершенно по-иному посмотреть на задачу согласования усилий всего мирового сообщества в решении данной проблемы.

В докладе Группы правительственных экспертов Организации Объединенных Наций (ООН) по достижениям в сфере информатизации и коммуникации в контексте международной безопасности отмечалось, что для успешного противодействия злонамеренному использованию информационно-коммуникационных технологий, создающему угрозу международному миру и безопасности, необходимы совместные меры государств – членов ООН и, в частности, выработка «общего понимания в отношении применения соответствующих норм международного права и вытекающих из них норм, правил и принципов ответственного поведения государств»[1].

Несмотря на очевидность экстерриториальных угроз для критической информационной инфраструктуры отдельного государства, до настоящего времени на международном уровне не существует единого документа, устанавливающего некие общие обязательства участников международных отношений по криминализации и пенализации неправомерных посягательств на информационные объекты особой важности.

Т. Л. Тропина метко указывает на эту проблему: «…имеющиеся международные инструменты, направленные на обеспечение кибербезопасности,

---

[1] Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. Записка Генерального секретаря ООН от 24 июня 2013 г. A/68/98. [Электронный ресурс]. URL: https://www.un.org (дата обращения: 12.02.2021).

характеризуются мозаичностью, являются фрагментарными и скорее конкурируют между собой, чем способствуют гармонизации уголовного и уголовно-процессуального законодательства государств»[1].

По мнению В. С. Овчинского, трудности национальных правительств в вопросах защиты собственного суверенного права на регулирование информационного пространства (включая национальный сегмент сети «Интернет») кроются в отсутствии международно-правовых механизмов. «Большинство государств (в том числе Россия), – отмечает автор, – вынуждены «на ходу» адаптировать государственное регулирование сферы информации и информационных технологий к новым обстоятельствам»[2].

В связи требуется не только оперативная корректировка и унификация нормативной правовой базы для обеспечения кибербезопасности на глобальном уровне, но и, как верно подчеркивает А. В. Серебренникова, крайне важно повышать эффективность международного сотрудничества[3].

В рамках Парижской цифровой недели 12 ноября 2018 г. на XIII Форуме по управлению Интернетом, проведенном в штаб-квартире ЮНЕСКО в Париже, Президент Франции Э. Макрон выступил с Парижским призывом к доверию и безопасности в киберпространстве. Участники Парижского призыва не только осудили противоправную деятельность, которая угрожает критическим информационным инфраструктурам, но и подчеркнули, что в целях обеспечения соблюдения прав граждан и их защиту в онлайн-пространстве, так же, как в реальной жизни, государства должны действовать сообща, привлекать партнеров из частного сектора, исследовательских кругов и гражданского общества.

В документе справедливо подчеркивается, что международное право, в том числе весь Устав ООН, международное гуманитарное право и международное

---

[1] *Тропина Т. Л.* Борьба с киберпреступностью: возможна ли разработка универсального механизма? // Международное правосудие. 2012. № 3. С. 86–95.

[2] *Овчинский В. С.* Криминология цифрового мира : учебник для магистратуры. М., 2018. С. 11.

[3] См.: *Серебренникова А. В.* Правовые основы кибербезопасности в Российской Федерации // Пробелы в российском законодательстве. 2021. № 4. С. 265.

обычное право, применимы при использовании государствами информационно-коммуникационных технологий (ИКТ); права, которые закреплены за всеми людьми вне онлайн-пространства, должны защищаться и внутри него; международное право прав человека применимо в киберпространстве; международное право вместе с добровольными нормами ответственного поведения государств в мирное время и мерами по развитию доверия и укреплению потенциала, разработанными в рамках ООН, составляют фундамент международного мира и безопасности в киберпространстве[1].

Документ был поддержан 58 странами, 115 международными и региональными организациями, 284 частными компаниями и корпорациями. (Российская Федерация не является подписантом Парижского призыва).

Парижский призыв демонстрирует не только понятную заинтересованность мирового сообщества в том, чтобы выработать специальные нормы международного права в сфере кибербезопасности. Немаловажно, что страны – подписанты Парижского призыва высказались положительно относительно того, что все наследие международного гуманитарного и международного обычного права применимо к отношениям, складывающимся в виртуальном пространстве. Иными словами, ранее принятые государствами обязательства по борьбе с преступлениями международного характера в равной мере распространяются и на их проявления в киберпространстве.

Акты международного сотрудничества, непосредственно направленные на противодействие неправомерному воздействию на КИИ, на наш взгляд, можно разделить на две группы:

1) международные документы первого поколения, направленные на гармонизацию усилий и законодательств государств в сфере противодействия киберпреступности в целом;

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

---

[1] URL: www.diplomatie.gouf.fr (дата обращения: 06.10.2022).

В ряду первой группы особое место должно быть отведено Конвенции о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.)[1] (далее — Будапештская конвенция), которая в Парижском призыве названа важнейшим инструментом стимулирования международного сотрудничества.

Следует согласиться с тем, что на настоящий момент данный международный документ является наиболее значимым с точки зрения консолидации усилий мирового сообщества в борьбе с компьютерной преступностью[2].

С 2001 года в рамках Содружества Независимых Государств (СНГ) действовало Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации (Москва, 1 июня 2001 г.). Основными целями сотрудничества в рамках данного соглашения было заявлено «обеспечение эффективной борьбы с преступлениями в сфере компьютерной информации» и «создание правовых основ сотрудничества правоохранительных и судебных органов стран – участников Соглашения» в борьбе с ними[3].

С 12 марта 2020 г. вступило в силу Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий (Душанбе, 28 сентября 2018 г.)[4], пришедшее на смену Соглашению от 2001 г. Следует согласиться с мнением отдельных авторов, что по сравнению с Соглашением СНГ 2001 г. и Будапештской конвенцией Соглашение СНГ 2018 г. представляется более лаконичным и современным международным правовым актом, который должным

---

[1] [Электронный ресурс]. Доступ из справ.-правовой системы «Консультант-Плюс».

[2] Конвенцию ратифицировали 29 из 47 государств – членов СЕ и США. Российская Федерация не ратифицировала ее из-за положений о трансграничном доступе к хранящимся компьютерным данным (п. «b» ст. 32).

[3] URL: www.mid.ru, 06.06.2001 (дата обращения: 06.12.2022).

[4] Единый реестр правовых актов и других документов СНГ. URL: http://cis.minsk.by (дата обращения: 02.02.2023).

образом адаптирован к особенностям национальных правовых систем государств данного региона[1].

Вместе с тем в Соглашении СНГ 2018 г. отсутствует специальное указание на необходимость криминализации неправомерного воздействия на критическую информационную инфраструктуру (что, несмотря на дату принятия документа, и обусловило отнесение этого Соглашения к международным актам первого поколения). Полагаем, что в этом аспекте Соглашение СНГ 2018 г., как основной документ о противодействии цифровой преступности в регионе, требует доработки — включения в ст. 3 пункта «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».

В ряду международных документов первого поколения можно также выделить Конвенцию о борьбе с преступлениями в области информационных технологий Лиги арабских государств от 21 декабря 2010 г.[2]. Особенностью данного документа, пожалуй, является специальное выделение в части рекомендаций по криминализации нормы о кибертерроризме (ст. 15).

Надо признать, что сама идея не является новой и для отечественной доктрины уголовного права. Вместе с тем возникают серьезные сомнения в целесообразности такой казуализации Особенной части УК РФ. Положения ст. 205 УК РФ характеризуются тем уровнем обобщения, который в полной мере позволяет осуществить надлежащий уголовно-правовой ответ на деяния, определяемые как «кибертерроризм».

Изложенное позволяет заключить, что международные акты первого поколения заложили основу противодействия преступлениям в сфере

---

[1] См., например: *Мысина А. И.* К вопросу о региональных правовых основах сотрудничества государств по противодействию преступлениям в сфере информационных технологий // Российская юстиция. 2019. № 5. С. 23.

[2] League of Arab States, 2010. Arab Convention on Combating Information Technology Offences. URL: http://www.arableagueonline.org (дата обращения: 20.02.2023).

компьютерной информации путем выделения своего рода базовых посягательств на безопасность информационных данных и компьютерных систем. При этом в них еще не была отражена проблема обеспечения повышенной защиты объектов информационной инфраструктуры особой важности.

В ряду международных документов второго поколения следует, прежде всего, выделить Резолюцию Генеральной Ассамблеи ООН от 21 декабря 2009 г. № 64/211 «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»[1]. В рамках данного документа было отмечено, что значительно возрос вклад сетевых информационных технологий «в выполнение многих важнейших функций в повседневной жизни, торговлю и обеспечение товарами и услугами, научные исследования, инновационную деятельность, предпринимательство и свободную передачу информации между физическими лицами и организациями, правительствами, деловыми кругами и гражданским обществом». Одновременно в Резолюции указывается, что «угрозы надежному функционированию важнейших информационных инфраструктур и целостности информации, передаваемой по этим сетям, приобретают все более изощренный и серьезный характер, отрицательно сказываясь на уровне семейного, национального и международного благополучия». Из значимых положений исследуемого международного документа следует также указать на положение о том, что «обеспечение защищенности важнейших информационных инфраструктур — это обязанность государства», и каждый участник международных отношений «вправе самостоятельно определять свои собственные важнейшие информационные инфраструктуры».

Далее следует назвать Соглашение между правительствами государств – членов Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.)[2]. В данном Соглашении (приложение 1 к ст. 1)

[1] Официальный сайт ООН. URL: www.un.org (дата обращения: 10.01.2023).
[2] Бюллетень международных договоров. 2012. № 1. С. 13–21.

уже закреплено определение критически важных структур — объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо затрагивающие национальную безопасность, включая безопасность личности, общества и государства. Значимым также является определение понятия «информационная война» — 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.

Соглашаясь с мнением отдельных специалистов о том, что на международных площадках до настоящего времени нет единства мнений о необходимости правового определения как самого состояния информационной войны (кибервойны), так и правил ее ведения[1], лишь дополним, что в данном случае требуется интенсификация международного правотворчества. Счет случаям неправомерного воздействия на КИИ отдельных стран со стороны правительственных организаций конкретного государства уже сейчас идет на десятки. Объективно это является проявлением прямого акта агрессии одного государства по отношению к другому. Вместе с тем имеющееся на уровне международного права определение войны не позволяет не только выразить адекватную правовую оценку таким деяниям, но и поставить вопрос о необходимости принятия соответствующих мер на уровне международных организаций, в том числе Совета безопасности ООН.

В связи с этим, на наш взгляд, отвечающим современным угрозам является дальнейшее совершенствование отечественного уголовного законодательства в части установления ответственности за преступления против мира и

---

[1] См., например: *Молчанов Н. А., Матевосова Е. К.* Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права // Актуальные проблемы российского права. 2020. № 1. С. 133–141.

безопасности человечества (гл. 34 УК РФ). Перспективным видится дополнение соответствующей главы УК РФ нормой, предусматривающей ответственность за планирование, подготовку, развязывание и ведение информационной войны.

В рамках Европейского союза (далее — ЕС, Евросоюз) было принято несколько международных документов, прямо или косвенно направленных на установление минимальных стандартов уголовно-правового противодействия атакам на КИИ.

В Директиве Европейского парламента и Совета ЕС от 12 августа 2013 г. № 2013/40/ЕС «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС»[1] (далее — Директива № 2013/40/ЕС) подчеркивается, что информационные системы являются ключевым элементом политического, социального и экономического взаимодействия (Преамбула).

В документе говорится о необходимости предусмотреть более суровые наказания за совершение атаки на информационную систему преступной организацией, как это определено в Рамочном решении 2008/841/ПВД Совета ЕС от 24 октября 2008 г. о борьбе с организованной преступностью[2], когда совершение компьютерных атак производится в *крупном масштабе* (выделено мной — *И. М.*), поражая тем самым значительное количество информационных систем, *в том числе когда она совершается посредством ботнета* (выделено мной — *И. М.*). Также целесообразно предусматривать более суровые наказания, когда атака совершается на объекты жизнеобеспечения государств – членов ЕС или Европейского союза в целом (Преамбула).

Здесь необходимо отметить, что Директива № 2013/40/ЕС задает сразу несколько направлений для дифференциации уголовной ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры:

---

[1] Official Journal of the European Union. № L 218, 14.08.2013. P. 8. URL: http://eur-lex.europa.eu.

[2] Текст документа официально опубликован не был [Электронный ресурс]. Доступ из справ.-правовой системы «КонсультантПлюс».

1) в зависимости от наличия определенной формы соучастия — организованной группы или преступного сообщества (преступной организации);

2) в зависимости от способа совершения посягательства — с использованием сети зараженных компьютеров (ботнета);

3) при наступлении тяжких последствий.

Изложенное дает основание сделать вывод, что модель дифференциации ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры, реализованная в ст. 274^1 УК РФ, требует своего переосмысления и доработки.

Особое внимание следует обратить на положения Директивы № 2013/40/ЕС, в которых разъясняется невозможность реализации уголовной ответственности в отношении лиц, совершивших деяния, объективно содержащие признаки преступлений, предусмотренных Директивой: 1) при отсутствии умысла, например, когда лицо не знает, что доступ не был разрешен, или 2) в случае санкционированной проверки или защиты информационных систем, при которых компания или разработчик поручают лицу проверить эффективность системы безопасности (ст.ст. 3–7).

С удовлетворением можно констатировать, что подобное правило об отсутствии признаков компьютерного преступления в случаях санкционированного тестирования системы на защищенность от проникновения, в том числе осуществляемого с использованием вредоносных компьютерных программ, получило свое закрепление в абз. 4 п. 11 постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37. Это значительный шаг в развитии отечественной доктрины уголовного права о преступлениях против информационной безопасности.

Относительно уголовно-правовой политики в сфере пенализации за подобные преступления Директива № 2013/40/ЕС определяет, что государства – члены Европейского союза должны принять необходимые меры по обеспечению наказуемости указанных преступлений посредством применения эффективных, соразмерных и оказывающих сдерживающее воздействие уголовных наказаний.

При этом государства-члены должны принять необходимые меры по обеспечению наказуемости указанных преступлений посредством применения максимального срока лишения свободы, равного *самое меньшее двум годам* (ст. 9).

В Директиве отдельно оговаривается, что участники Соглашения должны принять необходимые меры по обеспечению наказуемости преступлений, указанных в ст. 4 и 5 Директивы и совершаемых с умыслом, посредством применения максимального срока лишения свободы, равного *самое меньшее пяти годам,* если:

а) преступления совершены в рамках деятельности преступного сообщества;

б) причинили серьезный ущерб;

в) преступления совершаются против информационной системы инфраструктурного объекта жизнеобеспечения (ст. 9).

В 2014 году на пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ был принят Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры[1], в рамках которого нашли свое решение несколько вопросов, связанных, прежде всего, с определением понятийного аппарата — ст. 1:

- дано определение понятия «объект информационно-коммуникационной инфраструктуры», под которым понимается 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;

- закреплена классификация критически важных объектов информационно-коммуникационной инфраструктуры:

[1] Постановление Межпарламентской Ассамблеи государств – участников СНГ от 28 нояб. 2014 г. № 41-14 // Информационный бюллетень Межпарламентской Ассамблеи государств – участников СНГ. 2015. № 62, ч. 2.

а) объекты, которые обеспечивают функционирование экологически опасных и (или) социально значимых производств и (или) технологических процессов, нарушение или прекращение штатного режима которых может привести к чрезвычайной ситуации техногенного характера;

б) объекты, которые осуществляют функции информационной системы, нарушение или прекращение функционирования которой может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах;

в) объекты, которые обеспечивают предоставление значительного объема информационных услуг, частичное или полное нарушение или прекращение оказания которых «может привести к значительным негативным последствиям для национальной безопасности в политической, экономической, социальной, информационной, экологической, иных сферах».

Немаловажным представляется также то, что в Модельном законе сформулировано определение понятия «безопасность критически важных объектов информационно-коммуникационной инфраструктуры» — урегулированная законодательными актами система общественных отношений, которая обеспечивает охрану и защиту таких объектов, а также их работников от угроз, возникающих в связи с характером их деятельности, а также безопасное функционирование критически важных объектов информационно-коммуникационной инфраструктуры при реализации таких угроз.

Наконец, 25 октября 2019 г. Советом глав правительств СНГ в г. Москве было принято решение «О Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств»[1] (далее — Решение Совета СНГ о Стратегии обеспечения информационной безопасности).

В рамках данного документа обеспечение надежности и устойчивости функционирования объектов критической информационной инфраструктуры

[1] Единый реестр правовых актов и других документов СНГ. URL: http://cis.minsk.by (дата обращения: 20.06.2021).

отнесено к основным национальным интересам государств – участников СНГ в информационной сфере.

Как следует из Решения Совета СНГ о Стратегии обеспечения информационной безопасности, критическая информационная инфраструктура представляет собой совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации, являющихся жизненно важными для государства, отказ или разрушение которых может оказать существенное отрицательное воздействие на национальную безопасность.

Основными источниками угроз в отношении обеспечения безопасности информационных и телекоммуникационных средств и систем объектов критической информационной инфраструктуры, формирования системы обеспечения информационной безопасности, обеспечения защиты сведений, составляющих охраняемую законодательством тайну, определены:

- несанкционированный доступ к информационным ресурсам;

- воздействие на информационные системы с целью перехвата управления ими или блокирования их работы;

- отказы технических средств и сбои в работе программного обеспечения в информационных системах и сетях.

В качестве приоритетных направлений в реализации обеспечения безопасности информационных и телекоммуникационных средств и систем объектов критической информационной инфраструктуры указаны совершенствование нормативно-правовой базы государств – участников СНГ, регламентирующей защиту информационных отношений, соответствующих установленным требованиям безопасности.

Кроме того, стоит отметить, что Российская Федерация заключила несколько двусторонних соглашений, направленных в том числе на обеспечение безопасности объектов КИИ, в числе которых:

- Соглашение между Правительством Российской Федерации и Правительством Республики Куба «О сотрудничестве в области обеспечения международной информационной безопасности» (Гавана, 11 июля 2014 г.)[1],

- Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики «О сотрудничестве в области обеспечения международной информационной безопасности» (Москва, 8 мая 2015 г.)[2],

- Соглашение между Правительством Российской Федерации и Правительством Республики Индии «О сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий» (Гоа, 15 октября 2016 г.)[3],

- Соглашение между Правительством Российской Федерации и Правительством Южно-Африканской Республики «О сотрудничестве в области обеспечения международной информационной безопасности» (Сямэн, 4 сентября 2017 г.)[4].

Важно констатировать, что сегодня применимое к отношениям в киберпространстве обычное международное право пока партикулярно, действует только между ограниченным кругом государств, для которых складывается соответствующая практика в силу регионального (локального) сотрудничества.

В заключение данного параграфа представляется необходимым остановиться на его основных положениях и выводах.

1. Проведенное исследование позволило обосновать теоретическую классификацию 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;

---

[1] Бюллетень международных договоров. 2015. № 4. С. 58–64.
[2] Бюллетень международных договоров. 2016. № 11. С. 82–88.
[3] Бюллетень международных договоров. 2017. № 4.
[4] Официальный сайт МИД России: www.mid.ru (дата обращения: 10.09.2022).

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

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

3. Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий, являясь основным документом о противодействии цифровой преступности в регионе, требует доработки путем дополнения:

- статьи 1 определением понятия «объект информационно-коммуникационной инфраструктуры»;

- статьи 3 новым пунктом следующего содержания: «в[1]) 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».

4. Отвечающим современным угрозам является дальнейшее совершенствование отечественного уголовного законодательства в части установления ответственности за преступления против мира и безопасности человечества — гл. 34 УК РФ. Перспективным видится дополнение этой главы специальной нормой об ответственности за планирование, подготовку, развязывание и ведение информационной войны, определение которой уже зафиксировано в отдельных международных документах регионального уровня.

5. С учетом последних рекомендаций международных документов требует переосмысления модель дифференциации ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры, реализованная в ст. 274[1] УК РФ.

§ 3. Основные подходы к определению ответственности за преступления, связанные с неправомерным воздействием на критическую информационную инфраструктуру, в законодательстве зарубежных стран

Полноценное проведение сравнительного анализа зарубежного законодательства предполагает не только формально-юридический анализ отдельных норм, но и изучение практики их применения, актов судебного толкования, положений доктрины по проблеме и, в конце концов, самой правовой культуры конкретного общества, где реализуется норма. Все это, безусловно, учитывалось при написании данной части работы.

Вместе с тем, ввиду проблем поискового и языкового характера, преследующих любого автора-правоведа, который занимается компаративистикой, а также по причине самой ограниченности объема настоящего исследования, все же в большей степени фокус внимания был направлен на изучение именно нормативного материала. В этом плане, как справедливо отмечает А.В. Серебренникова, подходы законодателей зарубежных стран к определению критериев криминализации, описанию объектов и способов совершения преступлений в сфере цифровых технологий значительно разнится[1]. В связи с чем важно учесть эту специфику нормативного закрепления и описания параметров нового вида современной преступности в сфере информационных технологий.

Выбор стран не имел единого критерия. Прежде всего, цель состояла в изучении законодательных моделей стран-лидеров по глобальному индексу кибербезопасности (США, Сингапур, Великобритания, Франция, Латвия). В то же время нельзя было оставить без внимания и регионы, традиционно представляющие особый интерес именно для отечественной теории уголовного

---

[1] См.: *Серебренникова А. В.* Преступления в сфере цифровых технологий в законодательстве России и зарубежных стран : постановка проблемы // Кризисы мировой науки и техники : парадигмы дальнейшего развития. Материалы I Международной научно-практической конференции (20 апреля 2020 г.). Ростов-на-Дону : Издательство Южного университета ИУБиП, 2020. С. 62 – 67.

права и правоохранительной практики. Здесь речь идет о странах постсоветского пространства и, прежде всего, входящих в Содружество Независимых Государств.

Страны Америки

Соединенные Штаты Америки, пожалуй, были и являются ведущей страной в активном продвижении концепции обеспечения безопасности объектов КИИ как элемента обеспечения национальной безопасности в целом. Этому способствовало то обстоятельство, что США довольно рано столкнулись с организованными кибератаками на объекты КИИ что позволило выявить проблему уязвимости страны по отношению к таким инцидентам. Учитывая, что большая часть критически важных инфраструктур в США находится в частной собственности, с самого начала акцент был сделан на необходимости построения эффективного государственно-частного партнерства, чтобы обеспечить обмен информацией для эффективного реагирования и защиты от кибератак. С тех пор в США сложилась многоуровневая система управления кибербезопасностью, которая основывается на государственно-частном сотрудничестве.

С середины 1980-х годов в США начали принимать различные законы, связанные с обеспечением безопасности объектов КИИ . В 2009 году был создан Центр кибербезопасности и разработан Национальный план реагирования на киберинциденты, который обеспечил тренинг по кибербезопасности под названием «Кибершторм» при Министерстве обороны и Министерстве национальной безопасности США.

В 2013 году были приняты Указ и Директива (ЕО) 13636 и PDD-21 «Улучшение кибербезопасности критически важной инфраструктуры»[1], которая в целом была направлена на совершенствование системы обмена информацией о киберугрозах и уязвимостях критических инфраструктур.

В 2014 году был принят Закон о повышении уровня кибербезопасности, «Акт Патриота» (Patriot Act) США. В этом документе содержится определение

[1] Executive Order – Improving Critical Infrastructure Cybersecurity // The White House [Official website]. URL: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improvingcritical-infrastructure-cybersecurity (дата обращения: 11.09.2021).

критических инфраструктур. Это – «системы и ресурсы, физические или виртуальные, настолько значимые для США, что их разрушение или нарушение нормальной работы способно подорвать военно-политическую безопасность государства, экономическую стабильность, здоровье граждан и общественный порядок, или повлечь за собой несколько вышеуказанных факторов в любой комбинации»[1].

Указ Президента США № 13800 «Об усилении кибербезопасности федеральных сетей и критически важной инфраструктуры»[2] был принят для налаживания прочных партнерских отношений между федеральным правительством с государственными и местными органами власти и частными организациями для защиты важнейших информационных инфраструктур на фоне возрастающих угроз кибербезопасности.

Ответственность за неправомерный доступ к охраняемой компьютерной системе или информации предусмотрена § 1030 Свода законов США[3]. Указанные положения продублированы в законах отдельных штатов (например, гл. 41 Свода законов штата Арканзас, гл. 16 Свода законов штата Южная Каролина, гл. 815 Свода законов штата Флорида и др.).

Уголовный кодекс штата Луизина[4] содержит специальную статью об ответственности за неправомерное вмешательство в функционирование объектов критической инфраструктуры (ст. 14:61). Анализ данной нормы позволяет заключить, что она описывает действия, связанные с физическим доступом на соответствующие объекты[5].

---

[1] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT). Act of 2001. URL: https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (дата обращения: 26.06.2021)

[2] Executive Order 13800 – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. URL: https://www.govinfo.gov/content/pkg/DCPD-201700327/pdf/DCPD-201700327.pdf (дата обращения: 20.09.2021).

[3] URL: https://www.law.cornell.edu/uscode/text/18 (дата обращения: 06.05.2022).

[4] URL: https://law.justia.com/codes/louisiana/2015/code-revisedstatutes/title-14/rs-14-61 (дата обращения: 04.04.2022).

[5] Unauthorized entry of a critical infrastructure is any of the following: (1) The intentional entry by a person without authority into any structure or onto any premises, belonging to another, that constitutes in whole or in part a critical infrastructure that is completely enclosed by any type of physical barrier. (2) The use or attempted use of fraudulent documents for identification purposes to enter a

В 2009 году федеральное правительство **Канады** опубликовало Национальную стратегию по критически важной инфраструктуре вместе с поддерживающим Планом действий по критической инфраструктуре. Последний документ определяет 10 важнейших секторов: энергетика и коммунальные услуги, финансы, продовольствие, транспорт, правительство, информационные и коммуникационные технологии, здравоохранение, водоснабжение, безопасность и производство. Кроме того, в нем уточняется, что основная цель национальной стратегии состоит в повышении устойчивости критически важной инфраструктуры страны посредством достижения трех стратегических целей: налаживание партнерских отношений, внедрение подхода к управлению рисками и улучшение обмена информацией[1]. При этом само уголовное законодательство Канады не содержит специальных положений об ответственности за неправомерное вмешательство в функционирование объектов критической информационной инфраструктуры.

Страны Азии

Исследование законодательств стран Азиатского региона, пожалуй, следует начать с **Китайской Народной Республики** (далее также — КНР, Китай). Следует согласиться с Е. А. Русскевичем, который указывает, что «китайская модель уголовно-правового противодействия киберпреступности развивалась в три этапа: 1-й этап — защита критической информационной инфраструктуры (1997 г.); 2-й этап — расширение защиты информационных ресурсов частных лиц (2009 г.) и 3-й этап — установление ответственности провайдеров и виртуальных пособников (2015 г.)»[2].

---

critical infrastructure. (3) Remaining upon or in the premises of a critical infrastructure after having been forbidden to do so, either orally or in writing, by any owner, lessee, or custodian of the property or by any other authorized person. (4) The intentional entry into a restricted area of a critical infrastructure which is marked as a restricted or limited access area that is completely enclosed by any type of physical barrier when the person is not authorized to enter that restricted or limited access area.

[1] URL: https://www.canada.ca/en/services/defence/national_security/criticalinfrastructure.html (дата обращения: 06.05.2022).

[2] См.: *Русскевич Е. А.* Уголовная ответственность за преступления в сфере компьютерной информации по законодательству Китайской Народной Республики: сравнительно-правовой анализ // Журнал зарубежного законодательства и сравнительного правоведения. 2018. № 5. С. 113.

С 1997 года УК Китая[1] предусматривает самостоятельную норму (ст. 285), предусматривающую ответственность за неправомерный доступ к компьютерным системам, связанным с новейшими научно-техническими разработками страны или имеющим отношение к обеспечению госбезопасности или деятельности органов государственной власти.

Значимым отличием российского закона в сравнении с китайской моделью является то, что УК РФ предусматривает обязательность последствий (причинение вреда) для неправомерного доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 2 ст. 274[1]).

Акт **Южной Кореи** о защите информационной и коммуникационной инфраструктуры (2001 г.)[2] определяет, что «любое лицо, которое нарушает, парализует или разрушает критически важную информационную и коммуникационную инфраструктуру в нарушение ст. 12, подлежит наказанию в виде тюремного заключения с исправительными работами на срок не более 10 лет или штрафа в размере не более 100 млн вон» (ст. 28).

В соответствии со ст. 12 данного закона никто не должен совершать действия, подпадающие под действие любого из следующих подпунктов: 1) доступ к критически важной информации и инфраструктуре связи любым лицом, не имеющим полномочий на доступ, или модификация, уничтожение, блокирование или копирование хранимых данных любым лицом, превышающим его полномочия доступа; 2) уничтожение данных критически важной информационной и коммуникационной инфраструктуры посредством использования вредоносных компьютерных программ с намерением помешать работе критически важной информационной и коммуникационной инфраструктуры; 3) внезапная отправка большого количества сигналов

---

[1] Уголовный кодекс Китайской Народной Республики : принят на 5-й сессии Всекитайского собрания народных представителей шестого созыва 14 марта 1997 г. : по состоянию на 2016 г. [Электронный ресурс] // Посольство КНР в Российской Федерации : сайт. URL: www.ru.china-embassy.gov.ch (дата обращения: 22.10.2022).

[2] URL: https://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&_type=part&key=43 (дата обращения: 21.03.2023).

с намерением помешать работе критически важной информационной и коммуникационной инфраструктуры или вызвать ошибку в обработке информации с помощью таких средств.

Важно отметить, что в данной статье законодатель Кореи довольно удачно разделяет ответственность за неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее блокирование, и за совершение так называемых DOS-атак на информационные ресурсы. В отечественном уголовном законодательстве, как известно, данная проблема не имеет удовлетворительного решения. Высказываемые специалистами точки зрения сводятся либо к расширительному толкованию положений ст. 272 и ст. 274 УК РФ, либо к необходимости совершенствования уголовного закона. Полагаем, что без коррекции УК РФ здесь не обойтись.

Закон **Народной Республики Бангладеш** о цифровой безопасности (2018 г.)[1] представляет собой комплексный нормативный акт в сфере обеспечения информационной безопасности. Данный документ содержит как положения регулятивного, так и охранительного характера в части установления ответственности за отдельные преступления в сфере компьютерной информации.

В рамках исследуемой темы необходимо акцентировать внимание на следующем. Во-первых, Закон Бангладеш о цифровой безопасности содержит легальное определение критической информационной инфраструктуры — объявленная Правительством внешняя или виртуальная информационная инфраструктура, которая контролирует, обрабатывает, распространяет или сохраняет любую информацию, данные или электронную информацию, и в случае повреждения или критического воздействия может отрицательно повлиять на: 1) общественную безопасность, финансовую безопасность или общественное здоровье; 2) национальную безопасность, национальную целостность или суверенитет (п. «g» ст. 2 гл. 1)[2].

---

[1] URL: https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf (дата обращения: 22.03.2023).

[2] External or virtual information infrastructure declared by the Government that controls, processes, circulates or preserves any information-data or electronic information and, if damaged or

Во-вторых, в ст. 17 данного закона предусмотрена норма об ответственности за неправомерный доступ к объектам критической информационной инфраструктуры. В части 1 указанной статьи предусмотрена ответственность за несанкционированный доступ к объекту КИИ Республики Бангладеш (наказывается лишением свободы на срок до 7 лет со штрафом). В части 2 этой статьи установлена ответственность за те же самые действия, если они были сопряжены с причинением вреда охраняемым законом интересам или созданием угрозы причинения такого вреда (наказывается лишением свободы на срок до 14 лет со штрафом). В части 3 данной статьи установлена повышенная ответственность для лица, совершившего повторно или систематически (неоднократно) неправомерный доступ к объектам КИИ. Санкция за подобное преступление довольна строгая, хотя и имеет альтернативный характер, — пожизненное лишение свободы или значительный штраф.

Указание на объекты КИИ присутствует также в диспозиции ст. 27 Закона о цифровой безопасности Бангладеш, где регламентирована ответственность за кибертерроризм (наказывается лишением свободы на срок до 14 лет; при повторности — пожизненное лишение свободы).

Анализ положений законодательства Бангладеш о противодействии преступлениям, связанным с неправомерным воздействием на объекты КИИ, позволяет сделать следующие замечания.

Прежде всего, обращает на себя внимание, что Закон Бангладеш о цифровой безопасности (2018 г.) устанавливает ответственность за так называемое «чистое хакерство» — несанкционированный доступ к объектам критической инфраструктуры без последствий. Отечественный подход, как известно, этого не предполагает. При этом заметен весьма репрессивный курс законодателя Бангладеш при конструировании санкций за такие деяния — до пожизненного лишения свободы.

---

critically affected, may adversely affect: (i) public safety or financial security or public health, (ii) national security or national integrity or sovereignty.

Закон **Республики Филиппины** о предупреждении киберпреступности (2012 г.)[1] определяет критическую инфраструктуру как компьютерные системы и (или) сети, физические или виртуальные, и (или) компьютерные программы, компьютерные данные и (или) данные трафика, настолько важные для страны, что неспособность, разрушение или вмешательство в такие системы и информационные активы может оказать пагубное воздействие на безопасность, национальную или экономическую безопасность, здоровье и безопасность населения страны или любую комбинацию этих факторов[2]. Законодатель Филиппин также устанавливает повышенную ответственность за действия, выраженные в неправомерным доступе к компьютерной информации, если они были сопряжены с атаками на информационные системы особой важности.

По законодательству **Сингапура** ответственность за посягательства на нормальное функционирование объектов критической информационной инфраструктуры регламентирована в двух самостоятельных нормативных актах: Законе о неправомерном использовании компьютерных технологий (1993 г.)[3] и Законе о кибербезопасности (2018 г.)[4]

Закон Сингапура о неправомерном использовании компьютерных технологий устанавливает наказание в виде штрафа в размере до 100 тыс. дол. США или до 20 лет тюремного заключения. В статье 9 разъясняется, что компьютер должен рассматриваться как «защищенный компьютер», если лицо, совершившее преступление, заведомо знало или должно было допускать, что компьютер, программа или данные используются в сферах, связанных: а) с безопасностью, обороной или международными отношениями Сингапура;

---

[1] URL: www.ru-zahn-info-portal-de (дата обращения: 11.11.2022).

[2] Critical infrastructure refers to the computer systems, and/or networks, whether physical or virtual, and/or the computer programs, computer data and/or traffic data so vital to this country that the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters.

[3] URL: https://sso.agc.gov.sg/Act/CMA1993?ValidDate=20180831&ProvIds=pr9 (дата обращения: 04.02.2023).

[4] URL: https://sso.agc.gov.sg/Acts-Supp/9-2018/Published/20180312?DocDate=20180312 (дата обращения: 04.02.2023).

б) предоставлением услуг связи, банковских и финансовых услуг, коммунальных услуг, функционированием общественного транспорта; в) защитой общественной безопасности, включая системы, связанные с основными службами экстренной помощи, такими как полиция, гражданская оборона и медицинские службы.

Закон Сингапура о кибербезопасности (2018 г.) содержит составы преступлений, связанные с ненадлежащим исполнением правил и стандартов владельцами и операторами КИИ:

1) «уклонение от предоставления информации, позволяющей уполномоченному органу (Comissioner) принять решение об отнесении компьютерной системы к объектам критической информационной инфраструктуры» (ст. 8) — наказывается штрафом в размере до 100 тыс. сингапурских долларов или лишением свободы на срок до 2 лет;

2) «уклонение от предоставления информации о конструкции, конфигурации и безопасности критической информационной инфраструктуры; информации, которая может потребоваться уполномоченному органу (Comissioner) для определения уровня кибербезопасности критически важной информационной инфраструктуры» (ст. 10) — наказывается штрафом в размере до 100 тыс. сингапурских долларов или лишением свободы на срок до 2 лет;

3) «несообщение в течение 7 дней уполномоченному органу об изменениях, связанных с владением (включая любую долю в таком владении) критически важной информационной инфраструктуры» (ст. 13) — наказывается штрафом в размере до 100 тыс. сингапурских долларов или лишением свободы на срок до 2 лет»;

4) «уклонение от обязательного аудита состояния защищенности объектов критической информационной инфраструктуры» (ст. 15) — наказывается штрафом в размере до 100 тыс. сингапурских долларов или лишением свободы на срок до 2 лет;

5) уклонение владельца КИИ от участия в тестировании безопасности, если предписание о необходимости такого участия было предварительно

направлено в письменной форме уполномоченным органом (ст. 16) — наказывается штрафом в размере до 100 тыс. сингапурских долларов»;

6) «уклонение владельца критической информационной инфраструктуры от выполнения обязательных требований уполномоченного органа в условиях, требующих обнаружения и предупреждения угроз для национальной безопасности, обороны, международных отношений, экономики, общественного здравоохранения, общественной безопасности или общественного порядка Сингапура» (ст. 23) — наказывается лишением свободы на срок до 10 лет.

С юридико-технической точки зрения модель, реализованная законодателем Сингапура, представляется довольно удачной. Общий закон о противоправном использовании компьютерных технологий регламентирует ответственность за так называемые общеуголовные компьютерные преступления, которые могут быть совершены общим субъектом. В свою очередь Закон о кибербезопасности содержит составы преступлений со специальными субъектами, включенными в специфическую группу общественных отношений, связанных с владением и эксплуатацией объектов критической информационной инфраструктуры.

Законодательство **Королевства Саудовская Аравия** о противодействии киберпреступности (Anti Cyber Crime Law 2007) не содержит специальных указаний об объектах КИИ, однако ст. 7 Закона о борьбе с киберпреступностью предусматривает повышенную ответственность за совершение неправомерного доступа к правительственной сети и получение информации, которая была определена правительством Саудовской Аравии как требующая защиты от несанкционированного раскрытия по причинам национальной безопасности (наказывается лишением свободы на срок до 10 лет)[1].

В публикациях зарубежных специалистов отмечается, что информационные технологии сильно повлияли на арабский мир за последнее десятилетие. По различным оценкам киберпреступность ежегодно обходится Королевству в несколько миллиардов саудовских риалов. Каждый год жертвами

[1] URL: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx (дата обращения: 04.02.2023).

киберпреступлений становятся миллионы человек. В качестве наиболее серьезного инцидента приводится атака против государственной нефтяной компании Aramco: в августе 2021 г. более 30 тыс. компьютеров компании были поражены разрушительным вирусом. В результате атаки уничтожены данные и стерты жесткие диски компьютеров и, как считается, атака была нацелена на прекращение добычи нефти[1].

Страны Африки

Африка представляет собой регион активного роста. Континент характеризуется увеличением численности населения, ростом экономики и, как следствие, повышением глобального влияния. В регионе проживает порядка 1,5 млрд человек, средний возраст 19,5 лет — это самое молодое население в мире. Выдающаяся роль молодежи влечет за собой экспоненциальную «технологизацию» африканского общества, которая выражается в последовательном увеличении пользователей современными средствами интернет-коммуникации. На этом фоне развивается быстрорастущая электронная коммерция, которая по разным оценкам к 2025 г. может достичь примерно 75 млрд дол. США[2].

Как и во всем мире, в африканском регионе с приходом цифровизации широкое распространение получила киберпреступность. Проведенные социологические исследования показали, что только в Южно-Африканской Республике (ЮАР) 67 % взрослого населения сталкивались с проявлениями компьютерной преступности. При этом каждому потерпевшему от такого преступления нанесен ущерб в среднем в размере 274 дол. США в год[3].

Вместе с тем профессиональное сообщество отмечает, что Африка занимает периферийное положение и не является значительным источником угроз для

---

[1] Bushra Mohamed. Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future // Information and Knowledge Management. 2013. № 12 [Электронный ресурс]. URL: https://www.researchgate.net/publication/309040131_Cyber_Crime_in_Kingdom_of_Saudi_Arabia_The_Threat_Today_and_the_Expected_Future (дата обращения: 04.02.2023).

[2] URL: http://www.mckinsey.com/industries/high-tech/our-insights/lions-go-digital-theinternets-transformative-potential-in-africa (дата обращения: 08.02.2023).

[3] URL: https://us.norton.com/cyber-security-insights-2016 (дата обращения: 08.02.2023).

глобальной информационной безопасности (менее 1 % от общего числа фиксируемых глобальных атак в год)[1].

Уголовное законодательство стран африканского региона об ответственности за киберпреступления до настоящего времени находится в стадии своего становления. Так, по состоянию на апрель 2016 г. обзорный анализ законодательств 54 стран Африки свидетельствовал о том, что:

1) в 11 государствах действуют основные (базовые) положения материального уголовного права (Ботсвана, Гана, Замбия, Камерун, Кот-д'Ивуар, Маврикий, Мавритания, Нигерия, Сенегал, Танзания и Уганда);

2) в 12 государствах ответственность установлена частично (Алжир, Бенин, Гамбия, Зимбабве, Кения, Мадагаскар, Марокко, Мозамбик, Руанда, Судан, Тунис и Южная Африка);

3) в большинстве африканских государств (30) не было конкретных законодательных положений о киберпреступности.

Уголовный кодекс **Буркина Фасо**[2] содержит достаточно широкую систему преступлений в сфере компьютерной информации (ст.ст. 700-1–722-1). Вместе с тем каких-либо специальных положений об ответственности за неправомерное воздействие на критическую информационную инфраструктуру он не содержит. Лишь в ст. 721-8 предусмотрено, что лицо наказывается лишением свободы на срок от 11 до 21 года и штрафом в размере от 50 млн до 100 млн франков, если оно будет признано виновным в сознательном совершении акта вандализма в отношении инфраструктуры электронных коммуникаций. Анализ приведенной диспозиции не позволяет точно разрешить вопрос о том, подразумевает ли данная норма ответственность за физический или цифровой вандализм (повреждение, выведение из строя) объектов инфраструктуры электронных коммуникаций, либо она охватывает обе эти формы. Здесь необходимо лишь отметить, что ст. 721-8

---

[1] Cyber crime & cyber security: Trends in Africa. 2016 [Электронный ресурс]. URL: https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf (дата обращения: 08.02.2023).

[2] URL: www.policinglaw.info/assets/downloads/Code_pénal__de_Burkina_Faso_(2018).pdf (дата обращения: 08.02.2023).

УК Буркина-Фасо помещена в разделе и главе под названием «Преступления, совершаемые с помощью информационных и коммуникационных технологий». Это позволяет с определенной уверенностью утверждать, что причинение вреда объектам инфраструктуры электронных коммуникаций в ст. 721-8 УК Буркина Фасо предполагает в том числе и так называемый «кибервандализм» — нарушение функционирования системы путем осуществления неправомерного доступа к ней, использования вредоносных компьютерных программ и т. д.

Закон **Ботсваны** «О киберпреступности и компьютерных преступлениях» (2018 г.)[1] дает следующее определение критической национальной инфраструктуры — компьютер, системы, устройства, сети, программы или данные, в том числе национальных организаций по чрезвычайным ситуациям, которые настолько важны для Ботсваны, что неспособность, разрушение или вмешательство в такие системы и активы окажут ослабляющее воздействие на национальную безопасность, национальную экономическую безопасность, общественное здоровье и безопасность или сочетание любого из этих факторов. Ответственность за совершение неправомерного доступа к критической национальной инфраструктуре Ботсваны предусмотрена в ст. 13 (наказывается лишением свободы на срок до 5 лет).

Обращают на себя внимание сравнительно мягкие наказания за преступления в сфере компьютерной информации по законодательству Ботсваны: наиболее строе наказание за общее компьютерное преступление, связанное с несанкционированным доступом к охраняемой компьютерной информации частных лиц и организаций, не превышает одного года лишения свободы.

Важной особенностью ст. 13 Закона Ботсваны «О киберпреступности и компьютерных преступлениях» является закрепление специального положения о презюмируемой осведомленности виновного о характере объекта, в отношении которого была осуществлена компьютерная атака: «…Для целей любого судебного преследования в соответствии с настоящей статьей предполагается,

---

[1] URL: www.bocra.org.bw/sites/default/files/documents/18%20Act%2029-06-2018%20Cybercrime%20and%20Computer%20Related%20Crimes.pdf (дата обращения: 08.02.2023).

пока не будет доказано обратное, что лицо знало, что компьютер является частью важнейшей национальной инфраструктуры».

Закон **Замбии** «О неправомерном использовании компьютера в преступных целях»[1] не оперирует категорией «критическая информационная инфраструктура». Статья 10 устанавливает более строгую ответственность за неправомерный доступ к «защищенному компьютеру» в результате совершения любого из предусмотренных данным законом преступлений — лишение свободы на срок от 15 до 25 лет.

В этой же статье разъясняется, что компьютер должен рассматриваться как «защищенный компьютер», если лицо, совершившее преступление, знало или должно было разумно знать, что компьютер, программа или данные используются непосредственно в связи или необходимы для:

(a) обеспечения безопасности, обороноспособности или международных отношений государства;

(б) идентификации конфиденциального источника информации, относящегося к уголовному судопроизводству;

(c) предоставления услуг, напрямую связанных с инфраструктурой связи, банковскими и финансовыми услугами, коммунальными услугами, общественным транспортом или общественной инфраструктурой;

(d) хранения секретной правительственной информации, или

(e) защиты общественной безопасности и здоровья населения, включая системы, связанные с основными службами экстренной помощи, такими как полиция, гражданская оборона и медицинские службы.

Аналогичный подход реализован в Законе **Уганды** «О неправомерном использовании компьютерных технологий» (2011 г.)[2] — ст. 20 «Ужесточение наказания за правонарушения, связанные с защищенными компьютерами». Вместе с тем примечательной особенностью данной статьи является ее абсолютно

---

[1] URL: www.zambialii.org/zm/legislation/act/_2004/13/cmaca2004379.pdf (дата обращения: 08.02.2023).

[2] URL: www.nita.go.ug/sites/default/files/publications/Computer%20Misuse%20Act%20%202011%20%28Act%20No.%202%20of%202011%29.pdf (дата обращения: 08.02.2023).

определенная санкция — лицо, признанное виновным в совершении данного преступления, подлежит наказанию в виде пожизненного лишения свободы.

Закон **Кении** «О противоправном использовании компьютерных технологий и киберпреступности» (2018 г.)[1] определяет понятие критической информационной инфраструктуры следующим образом: информационная система, программа или данные, которые поддерживают или выполняют функцию в отношении национальной критической информационной инфраструктуры, и критической инфраструктуры — процессы, системы, объекты, технологии, сети, активы и услуги, необходимые для здоровья, безопасности, защищенности или экономического благополучия кенийцев и эффективного функционирования правительства[2].

В соответствии со ст. 21 названного Закона неправомерный доступ или неправомерное вмешательство в работу объектов критической информационной инфраструктуры наказывается лишением свободы на срок до 20 лет со штрафом. С юридико-технической точки зрения ст. 21 является нормой с ссылочной диспозицией, которая отсылает к положениям ст. 14 и ст. 17 этого же Закона.

Примечательной особенностью законодательства Кении является наличие специальной нормы — ст. 13 об ответственности владельца объекта КИИ или иного уполномоченного лица, контролирующего критически важную информационную инфраструктуру, за уклонение от предоставления информации, которая может потребоваться в течение определенного периода для аудита состояния критической инфраструктуры. За это деяние законом предусмотрено альтернативное наказание в виде штрафа в размере до 200 тыс. шиллингов или лишения свободы сроком до 5 лет.

---

[1] URL: www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018 (дата обращения: 08.02.2023).

[2] Critical information infrastructure system or data means an information system, program or data that supports or performs a function with respect to a national critical information infrastructure «critical infrastructure» means the processes, systems, facilities, technologies, networks, assets and services essentials to the health, safety, security or economic well-being of Kenyans and the effective functioning of Government.

Похожая норма предусмотрена также в Законе **ЮАР** «О кибербезопасности и киберпреступности» (2017 г.)[1]. В статье 11 данного нормативного акта предусмотрена ответственность владельца объекта КИИ или лица, контролирующего такой объект, за совершение следующих альтернативных деяний:

1) если соответствующее лицо не инициирует аудит критически важной информационной инфраструктуры в случаях, предусмотренных законом;

2) не уведомляет службу государственной безопасности в письменной форме о проверке критически важной информационной инфраструктуры, которая должна быть выполнена при отдельных компьютерных инцидентах;

3) не сообщает о результатах аудита в течение 40 дней, как предусмотрено законом, или не предоставляет в течение указанного периода времени дополнительную информацию, запрошенную службой государственной безопасности;

4) предоставляет заведомо ложную информацию о результатах аудита критически важной информационной инфраструктуры (предусмотрены штраф либо лишение свободы на срок до 2 лет).

Положения данной нормы основаны на ст. 58 указанного Закона, которая предусматривает обязательный аудит критически важных информационных инфраструктур для обеспечения соответствия директиве, изданной членом Кабинета министров, ответственным за государственную безопасность. Владелец или лицо, контролирующее критически важную информационную инфраструктуру, должны каждые 24 месяца проводить за свой счет аудит критически важной информационной инфраструктуры независимым аудитором с целью оценки соответствия установленным требованиям. Владелец объекта критически важной информационной инфраструктуры должен уведомить соответствующий орган государственной власти о дате, когда должна быть проведена проверка. Владелец, как и лицо, контролирующее критически важную

[1] URL: https://www.gov.za/sites/default/files/gcis_document/201703/b6-2017cybercrimes170221a.pdf (дата обращения: 08.02.2023).

информационную инфраструктуру, по завершении аудита должны сообщить в установленных форме и способом о результатах аудита. Уклонение от проведения аудита или несоблюдение различных нормативных положений статьи влечет за собой соответствующую уголовную ответственность.

Закон **Нигерии** «О киберпреступности» (2015 г.)[1] предусматривает специальную норму и повышенную ответственность за совершение любого предусмотренного данным законом преступления против объекта критической информационной инфраструктуры (ст. 5). Дифференциация уголовной ответственности и пенализация построены следующим образом:

1) простое неправомерное воздействие на критически важную информационную инфраструктуру влечет наказание в виде лишения свободы на срок до 10 лет;

2) совершение того же деяния, повлекшего за собой тяжкие телесные повреждения любому лицу, наказывается лишением свободы на срок до 15 лет;

3) совершение деяния в соответствии с ч. 1 данной статьи, повлекшее причинение смерти человеку, наказывается пожизненным лишением свободы[2].

Страны Европы

Начнем, пожалуй, с **Великобритании**, где Закон о неправомерном использовании компьютеров 1990 г. (Computer misuse act 1990)[3] с 3 мая 2015 г. был дополнен ст. 3 ZA «Несанкционированные действия, вызывающие или создающие риск серьезного ущерба».

Формально-юридический и системно-логический анализ данной нормы позволяет заключить, что она представляет собой квалифицированный состав

---

[1] URL: https://www.cert.gov.ng/ngcert/resources/CyberCrime_Prohibition_Prevention_etc_Act_2015.pdf (дата обращения: 11.02.2023).

[2] (1) Any person who with intent, commits any offence punishable under this Act against any critical national information infrastructure, designated pursuant to section 3 of this Act, shall be liable on conviction to imprisonment for a term of not more than 10 years without an option of fine. (2) Where the offence committed under subsection (1) of this section results in grievous bodily harm to any person, the offender shall be liable on conviction to imprisonment for a term of not more than 15 years without option of fine. (3) Where the offence committed under subsection (1) of this section results in the death of person(s), the offender shall be liable on conviction to life imprisonment.

[3] URL: www.legislation.gov.uk/ukpga/1990/18/section/3ZA (дата обращения: 11.02.2023).

преступления, связанный с посягательством на объекты КИИ (хотя данный термин непосредственно в тексте статьи и не используется). С юридико-технической точки зрения норма имеет нестандартную в отечественном представлении конструкцию. В подтверждение сказанного приведем текст данной статьи в адаптированном, но в максимально близком по структуре переводе:

«(1) Лицо признается виновным в совершении преступления, если

(a) это лицо совершает какие-либо несанкционированные действия в отношении компьютера;

(б) во время совершения действия лицо знает, что оно является несанкционированным;

(c) действие причиняет или создает значительный риск серьезного материального ущерба; а также

(d) лицо намеревается своими действиями причинить серьезный материальный ущерб или сознательно допускает причинение такого ущерба.

(2) Ущерб является «материальным» для целей настоящей статьи, если он –

(a) связан с нанесением ущерба благополучию людей;

(б) нанесением ущерба окружающей среде;

(c) нанесением ущерба экономике любой страны; или

(d) ущерба национальной безопасности любой страны.

(3) Для целей подпункта (2) (a) действие причиняет ущерб благополучию человека, только если оно вызывает

(a) гибель людей;

(б) человеческое заболевание или травму;

(c) нарушение снабжения деньгами, едой, водой, энергией или топливом;

(d) нарушение системы связи;

(e) нарушение работы транспортных средств; или

(f) сбои в предоставлении медицинских услуг.

(4) Для целей пункта (2) несущественно, причиняет ли действие ущерб –

(a) делает это напрямую;

(б) является единственной или основной причиной ущерба.

(5) В этом разделе –

(a) ссылка на совершение действия включает ссылку на побуждение к совершению действия;

(б) «действие» включает серию действий;

(c) ссылка на страну включает в себя ссылку на территорию и на любое место в стране или на части или на ее территории.

(6) Лицо, виновное в правонарушении в соответствии с этой статьей, подлежит (если не применяется подраздел (7)) наказанию в виде лишения свободы на срок до 14 лет или наказывается штрафом, или приговаривается и к тому и к другому наказанию.

(7) Если правонарушение согласно этому разделу совершено в результате действия, вызывающего или создающего значительный риск:

(a) серьезный ущерб человеческому благополучию, упомянутый в подпунктах (3) (a) или (3) (b), или

(б) серьезный ущерб национальной безопасности, –

лицо, виновное в преступлении, подлежит наказанию в случае осуждения по обвинительному приговору к пожизненному тюремному заключению или к штрафу, либо к тому и другому».

В отечественной теории уголовного права справедливо отмечается, что указанная норма тождественна по своей сути ст. 274[1] УК РФ[1].

Уголовное законодательство **ФРГ**[2] не содержит специальной нормы об ответственности за неправомерное воздействие на объекты КИИ. В то же время привлечение к уголовной ответственности за подобные действия реализуется посредством применения норм о компьютерном саботаже (ст. 303b) и нарушении работы телекоммуникационных систем (ст. 317). С юридико-технической точки зрения законодатель Германии избрал путь ужесточения ответственности за

---

[1] См., например: *Бегишев И. Р., Хисамова З. И.* Сравнительно-правовой анализ законодательства Великобритании и России в области противодействия преступлениям в цифровой сфере // Электронный научный журнал Байкальского государственного университета. 2019. № 3. URL: www.aljournal.net (дата обращения: 08.02.2023).

[2] Уголовный кодекс Федеративной Республики Германия (1871 г. с изм.) // Федеральный правовой портал «Юридическая Россия». URL: www.law.edu.ru (дата обращения: 11.02.2023).

посягательства на компьютерные данные, а равно информационно-коммуникационную инфраструктуру в ситуациях, когда:

1) деяние связано с вмешательством в процесс обработки данных, имеющий существенное значение для осуществления экономической деятельности или деятельности иных организаций. В этом случае оно наказывается лишением свободы на срок до 5 лет[1];

2) При этом лицо подлежит наказанию в виде лишения свободы на срок от 6 месяцев до 10 лет в особо серьезных случаях, когда деяние:

а) повлекло серьезные финансовые потери,

б) лицо действовало в составе организованной группы, целью которой являлось продолжающееся совершение компьютерного саботажа,

в) лицо тем самым поставило под угрозу снабжение населения жизненно важными товарами или услугами или создало угрозу безопасности ФРГ[2].

По мнению И. Г. Пыхтина, «…ст. 202а УК Германии касается только шпионажа и только в том случае, если доступ к критической информационной инфраструктуре защищен, а виновный преодолевает антивирусную защиту, установленную в инфраструктуре, в противном случае преступник окажется безнаказанным. Поэтому считать, что данная норма прямо направлена на защиту критической информационной инфраструктуры, нельзя»[3].

Как представляется, автор, делая верный вывод о том, что ст. 202а УК Германии не направлена непосредственно на защиту объектов КИИ, тем не менее использует ошибочную аргументацию. Во-первых, в самой статье ничего не говорится именно об антивирусной защите. К тому же не совсем понятен тезис

---

[1] If the data processing operation is of substantial importance for another's business, enterprise or an authority, the penalty is imprisonment for a term not exceeding five years or a fine.

[2] In especially serious cases under subsection (2), the penalty is imprisonment for a term of between six months and 10 years. An especially serious case typically occurs where the offender: 1. major financial loss, 2. acts on a commercial basis or as a member of a gang whose purpose is the continued commission of computer sabotage or 3. by committing the offence jeopardises the population's supply with vital goods or services or the security of the Federal Republic of Germany.

[3] *Пыхтин И. Г.* Обеспечение уголовно-правовой охраны национальных объектов критической информационной инфраструктуры Германии, Австрии, Швейцарии и Франции // Известия Юго-Западного государственного университета. История и право. 2019. Т. 9. № 2 (31). С. 110.

автора, что статья может быть применена «только в том случае, если доступ к критической информационной инфраструктуре защищен». Возникает вопрос — а разве возможна иная ситуация? С точки зрения регулятивного законодательства независимо от юрисдикции объекты критической информационной инфраструктуры имманентно предполагают принятие необходимых мер программно-технической защиты. В статье 202a УК Германии объекты критической информационной инфраструктуры не упоминаются вовсе — эта общая норма устанавливает ответственность за неправомерный доступ к компьютерной информации путем преодоления защиты (по сути, за в ней идет речь о шпионаже данных). На нее делается ссылка в норме о компьютерном саботаже (ст. 303b), в которой, собственно, и реализована изложенная выше дифференциация ответственности.

В Уголовном кодексе **Франции** (ст. 323-1)[1] ответственность за удаление или изменение данных, находящихся в информационной системе, либо за действия, повлекшие изменение работы автоматизированный системы обработки данных дифференцирована в зависимости от того, совершило ли лицо преступление против такой системы так называемого общего назначения (наказывается лишением свободы на срок до 5 лет и штрафом до150 тыс. евро) либо против информационной системы, внедренной государством (наказывается лишением свободы на срок до 7 лет и штрафом до 300 тыс. евро).

Аналогичные положения содержатся в § 126a УК **Австрии**[2] и ст. 615-ter. УК **Италии**[3].

Уголовный кодекс **Республики Мальта**[4] предусматривает уголовную ответственность за компьютерные преступления в ст.ст. 337-B–337-H. Глава представляет собой не только описание наказуемых деяний, но также включает нормы-дефиниции и положения, связанные с институтами соучастия и

---

[1] Уголовный кодекс Франции (1992 г. с изм.) // Российский правовой портал «Библиотека Пашкова». URL: www.constitutions.ru (дата обращения: 01.02.2023).

[2] URL: www.unodc.org/cld/document/aut/1974/austrian_penal (дата обращения: 21.02.2023).

[3] URL: www.europam.eu/?module=legislation&country=Italy (дата обращения: 05.02.2023).

[4] URL: www.legislationline.org/download/id/8555/file/Malta_Criminal_Code_amDec2019_en.pdf (дата обращения: 21.02.2023).

неоконченного преступления. В статье 337-F УК Мальты реализована дифференциация ответственности за совершение соответствующих посягательств, если они были связаны:

1) с нарушением деятельности правительства, ухудшением или прерыванием предоставления каких-либо общественных услуг или коммунальных услуг;

2) с причинением серьезного ущерба;

3) направлены на объекты КИИ;

4) с совершением в рамках преступной организации[1].

Лицо, признанное виновным в совершении квалифицированного компьютерного преступления, предусмотренного указанной нормой, подлежит наказанию в виде штрафа в размере от 500 евро до 150 тыс. евро или наказывается лишением свободы на срок от 12 месяцев до 10 лет.

Примечательно, что в законодательстве Мальты разделено вмешательство в функционирование объектов КИИ и совершение компьютерного преступления, которое было связано с воспрепятствованием нормальной деятельности органов власти, предоставлением социальных услуг и т. п. Полагаем, что причина такого подхода кроется не только в особенностях регулятивного законодательства Республики Мальта о критической информационной инфраструктуре, но и в представлении о том, что соответствующие последствия могут наступить и без целевой компьютерной атаки на представляющие особую важность информационные объекты.

И в завершение обзора законодательств отдельных европейских стран по исследуемой тематике отметим, что Уголовный кодекс **Польши**[2] устанавливает ответственность за удаление или модификацию информации на электронном

---

[1] «…constitutes an act which is in any way detrimental to any function or activity of Government, or hampers, impairs or interrupts in any manner whatsoever the provision of any public service or utility, whether or not such service or utility is provided or operated by any Government entity; causes serious damage; is committed against a critical infrastructure facility information system; (d) is committed within the framework of a criminal organisation within the meaning of Council Framework Decision 2008/841JHA of 24 October 2008 on the fight against organised crime».

[2] URL: www.legislationline.org/download/id/7354/file/Poland_CC_1997_en.pdf (дата обращения: 24.02.2023).

носителе, имеющую особое значение для национальной обороны, транспортной безопасности, деятельности правительства или другого государственного органа или местного самоуправления — ст. 269 (наказывается лишением свободы на срок от 6 месяцев до 8 лет).

Теперь перейдем к анализу законодательств стран ближнего зарубежья.

Страны СНГ

УК **Азербайджана**[1] предусмотрены специальные квалифицирующие признаки неправомерного доступа к компьютерной информации — ст. 271. Согласно закону, отягчающим обстоятельством выступает совершение деяния в отношении «инфраструктурных объектов общественного значения».

УК Республики Казахстан[2] решает задачу обеспечения высокой степени защищенности объектов КИИ путем конструирования квалифицированных составов преступлений в сфере информатизации и связи (гл. 7 УК Республики Казахстан «Уголовные правонарушения в сфере информатизации и связи»). В частности, ст. 205 устанавливается более строгая ответственность за «неправомерный доступ к охраняемой законом информации, если это деяние совершено в отношении «критически важных объектов информационно-коммуникационной инфраструктуры»». Аналогичным образом этот квалифицирующий признак включен в ст. 206 «Неправомерное уничтожение или модификация информации», ст. 207 «Нарушение работы информационной системы или сетей телекоммуникаций», ст. 208 «Неправомерное завладение информацией», ст. 209 «Принуждение к передаче информации», ст. 210 «Создание, использование и распространение вредоносных компьютерных программ и программных продуктов».

Примечательно, что УК Казахстана предусматривает сравнительно мягкие санкции за совершение подобных посягательств. Совершение неправомерного

---

[1] Уголовный кодекс Азербайджанской Республики от 30 дек. 1999 г. : по состоянию на 29 нояб. 2022 г. [Электронный ресурс] // ЭБД «Законодательство стран СНГ». URL: www.base.spinform.ru (дата обращения: 24.02.2023).

[2] Уголовный кодекс Республики Казахстан от 3 июля 2014 г. № 226-V ЗРК по состоянию на 5 нояб. 2022 г. [Электронный ресурс] // ЭБД «Законодательство стран СНГ». URL: www.base.spinform.ru (дата обращения: 24.02.2023).

доступа к объектам критической информационной инфраструктуры, согласно ч. 2 ст. 205 УК Казахстана, наказывается штрафом в размере до 200 месячных расчетных показателей либо исправительными работами в том же размере, либо привлечением к общественным работам на срок до 200 часов, либо арестом на срок до 50 суток, с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 2 лет или без такового.

Наиболее строгое наказание предусмотрено за совершенные в отношении КИИ принуждение к передаче информации и создание, использование и распространение вредоносных компьютерных программ и программных продуктов — наказываются ограничением свободы на срок от 3 до 7 лет либо лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового.

Определение критически важных объектов информационно-коммуникационной инфраструктуры закреплено в п. 24 ст. 1 Закона Республики Казахстан от 24 ноября 2015 г. № 418-V ЗРК (ред. от 5 ноября 2022 г.) «Об информатизации»: объекты информационно-коммуникационной инфраструктуры, в том числе информационно-коммуникационной инфраструктуры «электронного правительства», нарушение или прекращение функционирования которых приводит к чрезвычайной ситуации социального и (или) техногенного характера или к значительным негативным последствиям для обороны, безопасности, международных отношений, экономики, отдельных сфер хозяйства, инфраструктуры Республики Казахстан или для жизнедеятельности населения, проживающего на соответствующей территории[1].

Уголовные законы других стран – участников СНГ не предусматривают специальных положений об ответственности за неправомерное воздействие на критическую информационную инфраструктуру.

Завершая исследование, проведенное в рамках данного параграфа, полагаем необходимым сформулировать наиболее важные выводы.

---

[1] URL: www.base.spinform.ru (дата обращения: 24.02.2023).

1. По способу юридического закрепления уголовной ответственности за неправомерное воздействие на КИИ действующие уголовные законодательства зарубежных государств можно разделить на три группы:

- первую составляют страны, в которых этот вопрос решается путем законодательной регламентации только общих положений об ответственности за преступления в сфере компьютерной информации (Беларусь[1], Буркина Фасо, Канада, Узбекистан[2]);

- вторую группу образуют уголовные законодательства государств, в которых совершение деяния в отношении критической информационной инфраструктуры выступает квалифицирующим признаком преступлений в сфере компьютерной информации (Австрия, Азербайджан, Германия, Италия, Казахстан, Латвия, Франция);

- третью группу формируют уголовные законодательства стран, в которых выделяются специальные нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру (Ботсвана, Великобритания, Замбия, Кения, Мальта, Нигерия, США, Уганда).

2. Выявлена практика криминализации в зарубежном законодательстве нарушения требований в области обеспечения безопасности КИИ специальным субъектом – лицом, обязанным соблюдать эти правила в силу выполняемой им работы или занимаемой должности. 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 (Кения, Сингапур, ЮАР);

---

[1] Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З (с изм.) : [принят Палатой представителей 2 июня 1999 г. : одобрен Советом Республики 24 июня 1999 г. : ред. от 9 марта 2023 г.] // Законодательство стран СНГ : электронная база данных. URL: www.baze.spinform.ru (дата обращения: 04.04.2023).

[2] Уголовный кодекс Республики Узбекистан от 22 сент. 1994 г. № 2012-XII (с изм.) : ред. от 19 окт. 2022 г. // Законодательство стран СНГ : электронная база данных. URL: www.baze.spinform.ru (дата обращения: 04.04.2023).

3. Зарубежный опыт в части криминализации не «эксплуатационных», а регулятивных требований в области критической информационной инфраструктуры, представляет значительный теоретический интерес и практический потенциал для российской уголовной политики. Полагаем, что исследуемая ст. 274^1 УК РФ, равно как и ст. 274^2 УК РФ, не распространяют свое действие на возможные и имеющие место в объективной действительности случаи злоупотреблений лицами, наделенными управленческими функциями в организациях, владеющих объектами критической информационной инфраструктуры (уклонение от категорирования, занижение категории значимости, уклонение от сообщения о компьютерных инцидентах и т. п.).

Глава 2. Юридический анализ неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Предваряя осуществление юридического анализа конструктивных и квалифицирующих признаков состава неправомерного воздействия на КИИ России, видится возможным дать некоторое пояснение по поводу ее построения. Поскольку, как уже отмечалось, ст. 274[1] УК РФ представляет собой сочетание уголовно-правовых норм, предусмотренных ст.ст. 272, 273 и 274 УК РФ, не имеет прикладного исследовательского смысла фокусировать внимание на тех ее признаках, которые достаточно хорошо разработаны в уголовно-правовой отечественной теории в рамках общего учения об ответственности за преступления в сфере компьютерной информации. Исходя из этого, в рамках настоящей главы исследовательский интерес преимущественно будет обращен на те вопросы, которые, с одной стороны, выявляют специализацию данной нормы, а, с другой — не получили своего обстоятельного рассмотрения в отечественной науке уголовного права.

Следует также сразу оговориться, что некоторые выводы и рекомендации относительно понимания криминообразующих и квалифицирующих признаков исследуемой нормы, конечно же, могут восприниматься как дискуссионные. В этом смысле исследование было направлено на то, чтобы с максимально возможной проработкой доктринальных источников по теме и имеющихся в открытом доступе материалов правоприменения «определить позицию», то есть предложить решение, сформулировать квалификационный алгоритм, которые в наибольшей степени решали бы задачи, поставленные перед механизмом уголовно-правовой охраны.

§ 1. Уголовно-правовая характеристика объективных признаков неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Объект неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Познание содержания и особенностей объекта исследуемого преступления имеет, на наш взгляд, фундаментальное значение как для раскрытия и конкретизации его общественной опасности, так и для разрешения сугубо прикладных вопросов по непосредственному применению ст. 274^1 УК РФ. Именно в характеристике и содержании объекта неправомерного воздействия на КИИ России заложена та информация, осмысление которой позволяет, условно говоря, выразить формально-юридическую идентичность состава преступления.

Изучение современной юридической литературы позволяет сделать вывод, что вопрос об объекте неправомерного воздействия на КИИ России хотя и поставлен в ряду актуальных проблем отечественной науки, однако не нашел своего обстоятельного разрешения. Большинство специалистов раскрывают объект исследуемого преступления инерционно, опираясь на ранее сформулированные конструкции, выработанные и применяемые к остальным преступлениям в сфере компьютерной информации, ссылаясь на то, что специализация состава так или иначе упирается в особенности предмета посягательства. Однако общий вывод о содержании объекта, как правило, пока разрешен неудовлетворительно.

Сложности в определении объекта исследуемого преступления во многом объяснимы точной мыслью Е. Н. Карабановой: «… использование в современном уголовном праве категории "объект преступления" осложнено многообразием концепций содержания объекта преступления как социально-правового явления, терминологической близостью с другими понятиями и внутренней полисемией данного термина, что требует аккуратного и максимально точного его применения

с обращением в случае необходимости к краткому пояснению значения, придаваемого рассматриваемому термину»[1].

А. Н. Попов полагает, что непосредственным объектом преступлений, указанных в гл. 28 УК РФ, признаются «общественные отношения в информационной сфере, обеспечивающие состояние защищенности личности, общества и государства от информационных угроз»[2]. Неясным здесь видится и понимание информационной сферы, равно как и содержание отношений, возникающих в ней. Неопределенности также добавляет использование автором категории «информационная угроза», суть и смысл которой не улавливаются.

Довольно распространенным в отечественной теории уголовного права является подход, согласно которому объектом неправомерного воздействия на КИИ России выступает ее безопасность. Так, Е. А. Русскевич пишет, что «объектом преступлений, предусмотренных ст. 274[1] УК РФ, выступает безопасность критической информационной инфраструктуры Российской Федерации, то есть состояние ее защищенности от любого воздействия программными или программно-техническими средствами, которое способно привести к нарушению ее функционирования и (или) нарушению безопасности обрабатываемой ею информации»[3].

Серьезным недостатком такого определения объекта, на наш взгляд, является его очевидная неинформативность — объектом посягательства на КИИ выступает безопасность КИИ. Равным образом можно было бы утверждать, что объектом кражи телевизора выступает безопасность телевизора. Однако же, как известно, отечественная теория уголовного права предпочитает в этом вопросе более полное и обстоятельное разъяснение. Это не означает, что мы полагаем, будто при совершении исследуемого преступления безопасность объектов КИИ не страдает. Конечно же, страдает. Однако вопрос об объекте неправомерного

---

[1] *Карабанова Е. Н.* Понятие объекта преступления в современном уголовном праве // Журнал российского права. 2018. № 6. С. 77.

[2] См.: *Попов А. Н.* Преступления в сфере компьютерной информации : учеб. пособие. СПб. : Санкт-Петербургский юрид. ин-т (филиал) Ун-та прокуратуры РФ, 2018. С. 22–23.

[3] *Русскевич Е. А.* Уголовное право и «цифровая преступность»: проблемы и решения : монография. М., 2019. С. 139.

воздействия на объекты КИИ России нельзя упрощенно сводить к их безопасности, он гораздо более сложен и предполагает раскрытие содержания тех общественных отношений, которые самим своим существованием обязаны возникновению и функционированию соответствующих объектов.

Вместе с тем надо отметить, что данная позиция поддерживается и другими специалистами[1]. В этом же ключе в своей монографии Р. Р. Гайфутдинов обосновывает, что непосредственным объектом исследуемого преступления является безопасность критической компьютерной информации[2].

Еще более сомнительный подход в понимании объекта исследуемого преступления предлагает Ю. В. Трунцевский. Рассматривая особенности ответственности владельцев и эксплуатантов объектов критической информационной инфраструктуры по ч. 3–5 ст. 274[1] УК РФ, автор указывает: «объектом данного преступления выступают общественные отношения по *обеспечению правил* (выделено мной — *И. М.*) эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в вышеуказанных системах, а также правил доступа к указанным объектам»[3]. Но социальные связи никакие правила, конечно же, не обеспечивают. Напротив, правовые предписания, технические стандарты и прочие нормы как раз и направлены на то, чтобы оказывать непосредственное воздействие на отношения субъектов, формировать желаемые образцы поведения и искоренять негативные, препятствующие нормальному укладу общественной жизни и развитию человека. Поэтому считаем, что нельзя согласиться с такой «юридизацией» объекта исследуемого преступного посягательства.

Объект преступления, предусмотренного ст. 274[1] УК РФ, не могут составлять сами информационные системы, информационно-

---

[1] См., например: Уголовное право России. Общая и Особенная части : учебник / Под ред. д-ра юрид. наук, проф. В. К. Дуюнова. 6-е изд. М. : РИОР: ИНФРА-М, 2019. С. 664.

[2] См.: *Гайфутдинов Р. Р.* Квалификация преступлений против безопасности компьютерной информации : монограф. М., 2019. С. 74.

[3] *Трунцевский Ю. В.* Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99–106.

телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности. Такая трактовка, на наш взгляд, противоречит устоявшемуся в отечественной доктрине уголовного права соотношению объекта и предмета преступления.

Содержание объекта исследуемого преступления может быть успешно раскрыто только с учетом как положений Закона о безопасности КИИ России, так и обстоятельств, приведших к принятию данного нормативного акта.

Напомним, что в пояснительной записке к проекту этого закона было указано, что он его принятие обусловлено «осуществляемым в Российской Федерации переходом к информационному обществу, при котором подавляющее большинство систем принятия решений и бизнес-процессов в ключевых отраслях экономики и сфере государственного управления реализуются или планируются к реализации с использованием информационных технологий. В информационных системах хранятся и обрабатываются значительные объемы информации, в том числе касающейся вопросов государственной политики и обороны, финансовой и научно-технической сферы, частной жизни граждан. Одновременно информационные технологии повсеместно внедряются при построении автоматизированных систем управления производственными и технологическими процессами, используемых в топливно-энергетическом, финансовом, транспортном и других секторах критической инфраструктуры Российской Федерации».

Если мы соотнесем соответствующие положения со ст. 1 Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы[1], то будет справедливо под объектом преступления, предусмотренного ст. 274[1] УК

[1] Указ Президента Рос. Федерации от 9 мая 2017 г. № 203 [Электронный ресурс] // Официальный интернет-портал правовой информации www.publication.pravo.gov.ru, 10.05.2017.

РФ, понимать общественные отношения, непосредственно связанные с построением и развитием в России информационного общества, цифровой экономики и электронного правительства.

Избранный аксиологический подход к определению объекта неправомерного воздействия на КИИ выявляет, на наш взгляд, его действительное содержание. Объектом данного преступления выступают не правила, регламентирующие функционирование объектов КИИ, не безопасность, которая важна, но всегда имеет обеспечительный (вторичный) характер, а непосредственно те социальные связи, которые уже сложились и продолжают развиваться на основе формирования в Российской Федерации информационного общества, цифровой экономики и электронного правительства.

Особенностью содержания факультативного объекта неправомерного воздействия на КИИ России является его крайняя неоднородность. Принимая во внимание, что неправомерное воздействие на объекты КИИ может касаться отношений, связанных с эксплуатаций автоматизированных систем в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, говорить о каком-либо строго определенном факультативном объекте просто невозможно. Если все же попытаться выразить такой объект некой цельной конструкцией, полагаем, что будет наиболее правильным определить его как совокупность общественных отношений, обеспечивающих охраняемые законом интересы личности, общества и государства.

Понимание содержания и особых черт объекта преступления, предусмотренного ст. 274^1 УК РФ, во многом зависит от качественной разработки его предмета. В настоящем исследовании представляется возможным опустить подробное изложение положений отечественного учения о предмете преступления. Укажем лишь, что уже на протяжении нескольких лет в российской теории уголовного права сформировался подход о необходимости утверждения

статуса информации (в том числе компьютерной) как одной из разновидностей предмета преступления[1].

Действительно, в современном цифровом мире, когда активное распространение получили «облачные» технологии, привязка информации к какому-то материальному носителю приобретает очевидно искусственный характер.

В теории уголовного права распространена позиция, согласно которой предметом исследуемого преступления выступает охраняемая компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации[2].

Р. Р. Гайфутдинов уточняет, что в ч. 2 ст. 274[1] УК РФ «компьютерная информация как предмет посягательства дополняется указанием на еще один дополнительный признак — содержание ее в критической информационной инфраструктуре Российской Федерации. Таким образом, предмет рассматриваемого преступления характеризуется местом его расположения в компьютерной технике, компьютерной сети и т. д., относящейся именно к указанной инфраструктуре»[3].

Полагаем, что указанный подход определения предмета преступления является дискуссионным. Главным аргументом против такого подхода является то, что ст. 274[1] УК РФ описывает разные общественно опасные деяния. Рельефно это обнаруживается на сопоставлении ч. 1 данной нормы с ее частями 2 и 3. Создание и использование вредоносного программного обеспечения может и не предполагать фактического воздействия на объекты КИИ. В этом смысле более удачно предмет неправомерного воздействия на КИИ раскрывает Е. А. Русскевич: «Предметом преступления, предусмотренного ч. 1 ст. 274[1] УК РФ, является

---

[1] См., например: *Малышенко Д. Г.* Уголовная ответственность за неправомерный доступ к компьютерной информации : автореф. дис. … канд. юрид. наук 12.00.08. М., 2002. С. 19 ; *Бикмурзин М. П.* Предмет преступления: теоретико-правовой анализ. М., 2006. С. 117.

[2] См., например: Уголовное право России. Общая и Особенная части : учебник / Под ред. д-ра юрид. наук, проф. В. К. Дуюнова… С. 664.

[3] *Гайфутдинов Р. Р.* Квалификация преступлений против безопасности компьютерной информации : монограф. … С. 80–81.

компьютерная информация или компьютерные программы, заведомо предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры. Специфическим предметом преступлений, предусмотренных частями 2 и 3 ст. 274[1] УК РФ, выступают объекты критической информационной инфраструктуры — информационные системы, информационно-телекоммуникационные сети государственных органов, а также информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления технологическими процессами, функционирующие в оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике, топливной, атомной, ракетно-космической, горнодобывающей, металлургической и химической промышленности»[1].

В приведенной позиции Е. А. Русскевича представляется дискуссионным отнесение к предмету исследуемого преступления компьютерных программ и компьютерной информации, заведомо предназначенных для осуществления вмешательства в функционирование объектов критической информационной инфраструктуры. Полагаем, что такие вредоносные программы не имеют непосредственной связи и не выражают охраняемые ст. 274[1] УК РФ общественные отношения, то есть объект неправомерного воздействия на КИИ. Здесь мы касаемся дискуссии относительно разграничения предмета преступления от орудий и средств его совершения, имеющей место в отечественной науке уголовного права уже на протяжении длительного времени. Не претендуя на решение столь сложной теоретико-правовой задачи в рамках настоящего исследования, позволим себе сделать вывод, что такие чуждые объекту уголовно-правовой охраны предметы, как вредоносные программы и вредоносная компьютерная информация, выступают средством его совершения и не могут быть отнесены к предмету преступления, предусмотренного ст. 274[1] УК РФ.

---

[1] *Русскевич Е. А*. Уголовное право и «цифровая преступность»: проблемы и решения: монограф. ... С. 140.

Довольно сложным вопросом представляется определение индивидуализирующих признаков вредоносной компьютерной программы и компьютерной информации, указанных в ч. 1 ст. 274[1] УК РФ. В диспозиции статьи закреплено, что такие программа и информация должны быть «заведомо предназначены» для осуществления противоправного воздействия на объект критической информационной инфраструктуры Российской Федерации. Здесь возникает расхождение в понимании этого признака: с одной стороны, можно говорить о том, что такие программа и информация должны с точки зрения своего содержания и функционала обладать уникальностью действия именно в отношении объектов критической информационной инфраструктуры и, с другой стороны, эту предназначенность можно также понимать как фактическую эффективность (применимость) программы против того или иного критически важного объекта, хотя в целом «вредоносность» может иметь широкий спектр действия и не обладать какой-либо внутренней спецификой.

На наш взгляд, второй подход противоречит самому смыслу появления ч. 1 ст. 274[1] УК РФ. Отечественный законодатель стремился к тому, чтобы дифференцировать ответственность именно за создание, распространение и использование не универсальных вредоносных программ, а именно тех из них, которые были изначально разработаны для совершения информационных атак на критически важные объекты.

Представители профессионального сообщества в сфере IT-безопасности довольно скептически оценивают вероятность появления именно уникальных вредоносных компьютерных программ, специально рассчитанных на осуществление атак в отношении объектов критической информационной инфраструктуры. Они утверждают, что функционал по преодолению средств программно-технической защиты почти всегда будет эффективен для совершения проникновений как к критически важным объектам, так и к оборудованию (устройствам) частных лиц. Однако же при этом интервьюеры соглашаются, что

в истории такие прецеденты имели место (здесь, как правило, упоминается известный факт о срыве иранской ядерной программы)[1].

Неопределенность признаков программы и информации, указанной в ч. 1 ст. 274[1] УК РФ, вызывает ошибочные решения на правоприменительном уровне. Так, по данной норме были квалифицированы действия медицинской сестры, которая внесла заведомо ложные сведения о вакцинации граждан в Единую государственную информационную систему Минздрава России. Органы предварительного следствия обосновали свое решение тем, что такие недостоверные данные являются компьютерной информацией, предназначенной для неправомерного воздействия на критическую информационную инфраструктуру. Суд совершенно справедливо не согласился с таким прочтением ч. 1 ст. 274[1] УК РФ и указал, что подсудимая не создавала вредоносную компьютерную информацию, а лишь вводила ложные сведения о вакцинированных гражданах с целью получения родственниками и знакомыми сертификатов о вакцинации. Подсудимая по предъявленному обвинению в совершении преступления, предусмотренного ч. 1 ст. 274[1] УК РФ, была оправдана[2].

Полагаем, что в анализируемом случае была дана неверная оценка совершенному деянию. Поведение соответствующего субъекта, допущенного к работе с категорированной базой данных, образует нарушение правил эксплуатации средств хранения охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре (ч. 3 ст. 274[1] УК РФ). В тех же случаях, когда медицинский работник не был допущен к работе в системе, но, используя сетевые идентификаторы другого пользователя и фактический доступ к компьютерному оборудованию, внес сведения о

[1] Информация получена лично соискателем в ходе интервью, неоднократно проводимых в кулуарах конференций.

[2] Приговор Брянского районного суда Брянской области от 28 апр. 2022 г. по делу № 1-14/2022 [Электронный ресурс] // Судебные решения РФ : сайт. URL: www.судебныерешения.рф (дата обращения: 25.10.2022).

фиктивной вакцинации, содеянное необходимо квалифицировать как неправомерный доступ к компьютерной информации (ч. 2 ст. 274[1] УК РФ)[1].

Изучение нормативных актов в сфере регулирования КИИ России позволяет сделать вывод, 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:

1) *критерием значимости*, то есть социальной, политической, экономической, экологической или оборонной (для безопасности государства и правопорядка) важности (ст. 7 Закона о безопасности КИИ России);

2) *реестровым критерием*, связанным с включением объекта в реестр значимых объектов критической информационной инфраструктуры (ст. 8 Закона о безопасности КИИ России).

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

Полагаем, что такой вывод о предмете преступления в наибольшей степени соответствует направленности деяния, описанного в ст. 274[1] УК РФ, в том числе с учетом конструкции исследуемого состава преступления, которая предполагает наступление общественно опасных последствий в виде причинения вреда КИИ России.

Возникает вопрос относительно квалификации действий лица, направленных на вмешательство в функционирование программных или программно-аппаратных средств, которые субъектом еще не были категорированы и, соответственно, не были включены ФСТЭК России в реестр значимых объектов КИИ. Здесь, на наш взгляд, следует руководствоваться

---

[1] См., например: Приговор Армянского городского суда Республики Крым от 19 окт. 2022 г. по делу № 1-89/2022 [Электронный ресурс] // Судебные решения РФ : сайт. URL: www.судебныерешения.рф (дата обращения: 28.10.2022).

следующим правилом: если на момент совершения общественно опасного деяния соответствующий объект не был включен в реестр значимых объектов КИИ, содеянное не может оцениваться в рамках ст. 274[1] УК РФ. Данным правилом необходимо руководствоваться и при разрешении вопросов об обратной силе уголовного закона.

В процессе настоящего исследования выяснилось, что толкование предмета преступления, предусмотренного ст. 274[1] УК РФ, вызывает некоторые затруднения в правоприменительной практике.

Так, по одному из дел суд указал: «…Г., действуя умышленно, достоверно зная, что *ПАО "Ростелеком" относится к объекту критической информационной инфраструктуры* (выделено мной — *И. М.*), используя свое служебное положение, осознавая противоправность и общественную опасность своих действий… осуществила неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, содержащейся в БД "Авалон" и хранящейся на защищенных сетевых ресурсах ПАО "Ростелеком"»[1].

Здесь суд допускает неточность, указывая, что ПАО «Ростелеком» является объектом критической информационной инфраструктуры, тогда как этот оператор связи является субъектом, а не объектом критической информационной инфраструктуры. Соответственно, предметом данного преступления выступают системы управления сетями этого оператора, то есть в приведенном выше примере — БД «Авалон».

Надо признать, что в правоприменительной практике можно найти и иные подходы к решению обозначенного вопроса, когда объектом критической инфраструктуры признаются все без исключения информационные системы субъекта, независимо от их категорирования и участия в обеспечении критических процессов.

---

[1] Приговор Ленинского районного суда г. Владивостока от 25 сент. 2019 г. по делу № 1-368/2019 [Электронный ресурс] // Судебные решения РФ : сайт. URL: www.судебныерешения.рф (дата обращения: 30.10.2022).

К примеру, по одному из уголовных дел представитель ФСТЭК России отметил, что «…ПАО "МТС" является субъектом критической информационной инфраструктуры Российской Федерации, а информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере связи, принадлежащие Обществу на законном основании, — объектами критической информационной инфраструктуры, независимо от того, закатегорированы ли они или нет… Если даже объект критической информационной инфраструктуры не обеспечивает критические процессы, он не перестает быть объектом критической информационной инфраструктуры, поэтому составление перечня объектов критической информационной инфраструктуры не нужно путать с перечнем объектов критической информационной инфраструктуры, подлежащих категорированию»[1].

Таким образом, изучение судебной практики в целом подводит к мысли о том, что при установлении предмета посягательства в соответствии со ст. 274[1] УК РФ суды, как правило, ориентируются на официальный ответ ФСТЭК России о включении соответствующей системы (ресурса, базы данных и т. п.) в реестр значимых объектов критической информационной инфраструктуры. Иная практика единична.

Довольно сомнительной представляется мысль о том, что *любая* информационная система крупной компании – субъекта критической информационной инфраструктуры, в том числе не обеспечивающая осуществление критически важных процессов, будет признаваться предметом преступления, предусмотренного ст. 274[1] УК РФ. При таком подходе теряется социально-правовой смысл данной нормы, ее дифференцирующее значение.

И. Р. Бегишев справедливо подчеркивает, что перечень отраслей, в которых могут быть выделены объекты КИИ, является искусственно ограниченным. Автор

---

[1] Апелляционное определение Астраханского областного суда от 14 апр. 2022 г. № 22-787/2022 [Электронный ресурс] // Судебные и нормативные акты РФ : сайт. URL: www.sudact.ru (дата обращения: 05.11.2022).

пишет, что «можно выделить и другие сферы экономической деятельности, например, жилищно-коммунальное хозяйство, строительство, сельское хозяйство, пищевая промышленность и т. д., которые следовало бы отнести к критической информационной инфраструктуре. В отношении таких объектов также возможны компьютерные атаки»[1].

Здесь мы можем только согласиться с автором. Действительно, совершение компьютерных атак на автоматизированные системы управления, например, в сфере пищевой промышленности, может вызвать не меньшие негативные последствия, чем на транспорте или в сфере связи. С учетом этого полагаем, что необходимо дополнить п. 8 ст. 2 Закона о безопасности КИИ в России, изложив его 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»[2].

---

[1] *Бегишев И. Р.* Безопасность критической информационной инфраструктуры Российской Федерации // Безопасность бизнеса. 2019. № 1. С. 27–32.

[2] Данный вывод нашел свою поддержку у 64 % опрошенных респондентов (см. приложение Б, с. 189–193).

Объективная сторона неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Познание признаков объективной стороны конкретного преступления является крайне важной задачей, поскольку именно характеристика деяния во многом определяет сущность конкретного посягательства. Следует сразу оговориться, что применительно к исследуемой норме это представляет нетривиальную задачу хотя бы по причине ее строения, связанного с объединением различных видов компьютерных преступлений.

В части 1 ст. 274^1 УК РФ предусмотрено деяние, аналогичное тому, что указано в ст. 273 УК РФ; его содержание состоит «в создании, использовании или распространении вредоносных компьютерных программ или информации, заведомо предназначенных для совершения атак на объекты критической информационной инфраструктуры». В целом толкование данных посягательств на информационную безопасность было осуществлено Пленумом Верховного Суда РФ в Постановлении № 37/2022. Вместе с тем необходимо оговорить отдельные наиболее спорные аспекты.

Так, *создание* предполагает совершение лицом действий, направленных на получение соответствующего вредоносного программного обеспечения, в том числе путем модификации других компьютерных программ или компьютерной информации. Привлечение к уголовной ответственности за данное преступление возможно при условии, что лицо полностью выполнило все необходимые действия по написанию алгоритма. При совершении преступления групповым способом лицо может написать лишь часть вредоносного кода, что, однако, не исключает его полной ответственности за конечный результат.

В этом отношении необходимо выработать позицию относительно распространенного подхода, согласно которому характер хранения вредоносных компьютерных программ для квалификации содеянного не имеет решающего

значения — вредоносная программа может быть записана в памяти компьютера, а равно и на иных носителях (в том числе и на бумаге)[1].

Критику такому подходу можно найти в работе Е. А. Русскевича и А. С. Мельникова: «…описание алгоритма на естественном языке, а не на языке программирования, выступает лишь одним из этапов создания программы. В связи с этим напрашивается закономерный вывод, что сама по себе идея (концепция, проект и т. п.) вредоносной программы, выраженная на листе бумаге, не есть программа как таковая. Не станем же мы оценивать как оконченное изготовление оружия создание его сборочного чертежа с разнесенными составными частями (взрыв-схемы)? Таким образом, определение целей компьютерного вируса, разработка его алгоритма и последующие действия по программированию правильнее оценивать как покушение на создание вредоносной программы. Создание вредоносной компьютерной программы следует считать оконченным с момента придания ей такого состояния, при котором она уже обладает соответствующим деструктивным функционалом (вредоносными свойствами) и пригодна для использования»[2].

С приведенным толкованием можно, пожалуй, согласиться. Полное описание вредоносной компьютерной программы на бумаге, совершение действий по программированию без получения итогового (пригодного для использования) компьютерного кода, по смыслу ч. 1 ст. 274[1] УК РФ, не может оцениваться как оконченное дейтвие по созданию программы.

Использование заключается в непосредственном применении вредоносной компьютерной программы для уничтожения, блокирования, модификации, копирования информации, а также для нейтрализации средств ее защиты.

По смыслу ст. 274[1] УК РФ невозможно оценивать как использование действия лица, выражающиеся в хранении и изучении вредоносной

---

[1] Методические рекомендации Генеральной прокуратуры Российской Федерации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. М., 2013. С. 9.

[2] См.: *Русскевич Е. А., Мельников А. С.* Об отдельных проблемах квалификации создания, использования и распространения вредоносных компьютерных программ // Российский следователь. 2018. № 8. С. 63.

компьютерной программы, а также в ее тестировании, направленном на установление особенностей ее функционирования и (или) на получение информации о возможном разработчике и т. п.

Важным в понимании использования по ч. 1 ст. 274[1] УК РФ является ответ на следующий вопрос: если использование учтено в конструкции ч. 2 ст. 274[1] УК РФ, в каком случае лицо может нести ответственность за данное деяние обособленно, в отрыве от неправомерного доступа к компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации? Во-первых, ничто не исключает возможность использования вредоносных компьютерных программ, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру, для выполнения компьютерных атак на аккаунты частных лиц и организаций. В таком случае содеянное необходимо квалифицировать по ст. 272 УК РФ и ч. 1 ст. 274[1] УК РФ. Во-вторых, использование таких программ может быть сопряжено с нарушением специальным субъектом правил эксплуатации по ч. 3 ст. 274[1] УК РФ, которая не охватывает ч. 1 ст. 274[1] УК РФ.

Под *распространением* следует понимать предоставление доступа к соответствующим программам или информации третьим лицам, а также их скрытую рассылку или размещение на интернет-ресурсах для осуществления компьютерных атак на объекты КИИ. Таким образом, распространение может выражаться в продаже вредоносного софта, в его безвозмездной передаче из корпоративной (хактивистской) солидарности, а также в совершении действий, направленных на заражение вредоносной компьютерной программой объектов критической информационной инфраструктуры.

В том случае, если лицо одновременно разработало, использовало и распространило вредоносную компьютерную программу, заведомо предназначенную для совершения компьютерных атак на объекты критической информационной инфраструктуры, содеянное следует оценивать как единое преступление.

Здесь важно сделать оговорку относительно того, что признаки сложного единичного преступления с альтернативными действиями не всегда могут иметь место в случае обнаружения на оборудовании виновного нескольких вредоносных цифровых объектов. В этом смысле следует установить самым подробным образом особенности субъективной стороны виновного. В тех случаях, когда лицо выступало разработчиком у разных заказчиков и осуществляло соответствующие действия в отношении разных объектов критической информационной инфраструктуры, довольно сложно говорить о возможности использования такого подхода, который, в частности, стал общепринятым по делам о незаконном хранении оружия (ст. 222 УК РФ). Как известно, незаконное приобретение виновным новой единицы оружия весьма незначительно сказывается на объекте уголовно-правовой охраны.

В то же время, когда лицо является разработчиком и (или) эксплуатантом разных видов вредоносного программного обеспечения, заведомо применяемого по разным объектам критической информационной инфраструктуры в сфере обороны, здравоохранения, транспорта и т. п., уже нельзя согласиться с правильностью квалификации содеянного как единичного преступления. Поэтому, на наш взгляд, создание, использование и распространение по смыслу ст. 274[1] УК РФ образуют единое посягательство только в том случае, когда они осуществляются для создания угрозы одному конкретному объекту критической информационной инфраструктуры.

По мнению Р. Р. Гайфутдинова, под неправомерным воздействием на КИИ следует также понимать распространение содержащейся в ней информации[1]. Полагаем, что для столь расширительного толкования диспозиции исследуемого преступления нет достаточных оснований. Конечно же, можно поставить вопрос об общественной опасности таких действий и необходимости изменения отечественного уголовного законодательства в данном аспекте (хотя они чаще

[1] См.: *Гайфутдинов Р. Р.* Квалификация преступлений против безопасности компьютерной информации : монограф. … С. 83.

всего будут подпадать под признаки составов преступлений, предусмотренных ст.ст. 137, 183, 275, 276 УК РФ и др.).

Объективная сторона преступления, предусмотренного ч. 2 ст. 274[1] УК РФ, заключается в неправомерном доступе к компьютерной информации, содержащейся в критической информационной инфраструктуре, то есть в совершении лицом действий, связанных с получением непосредственного доступа к соответствующей информации путем нейтрализации средств ее программно-технической защиты либо иным несанкционированным способом без согласия владельца (оператора) данных.

Можно сказать, что «ахиллесовой пятой» уголовно-правовой нормы об ответственности за неправомерное воздействие на объекты КИИ России является указание на причинение вреда как на обязательное общественно опасное последствие совершенного деяния. Законодатель, конечно, в этом вопросе прибегнул к максимально возможной абстракции в описании последствий преступления. Это, по нашему мнению, весьма спорное решение.

Ю. В. Трунцевский пишет о том, что «законодатель вполне логично ставит ответственность в зависимость от наступления общественно опасных последствий преступления, предлагая судебной системе самостоятельно определять порог размера малозначительности причиненного вреда»[1]. Понятно, что таким образом достигается весьма существенная «гибкость» механизма уголовно-правовой охраны. Вместе с тем также и очевидно, что этот признак будет постоянным поводом для дискуссий в судах и, что более значимо, возможностью для злоупотреблений на уровне правоприменения. К сожалению, понимание содержания данного признака не было представлено и в постановлении Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37.

Доктрина уголовного права демонстрирует разные попытки внести ясность в определение вреда по смыслу ст. 274[1] УК РФ. Так, Е. А. Русскевич и И. Г.

---

[1] См.: *Трунцевский Ю. В*. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 103.

Чекунов в разрешении данного вопроса предлагают опираться на понятие компьютерного инцидента, сформулированного п. 5 ст. 2 Закона о безопасности КИИ России[1].

Складывающаяся в это же самое время судебная практика позволяет выделить следующие подходы к пониманию вреда как признака неправомерного воздействия на критическую информационную инфраструктуру:

1) «модификация информации в базе данных посредством внесения в нее недостоверной информации, что нарушило целостность информационной системы, в результате чего информация, циркулирующая в ней, перестала соответствовать критериям оценки объективности, достоверности и актуальности»[2];

2) «нарушение состояния защищенности и конфиденциальности сведений, содержащихся в критической информационной инфраструктуре»[3];

3) «изменение конфигурации элементов информационной системы субъекта критической информационной инфраструктуры, нарушение процесса предоставления услуг связи абонентам»[4] и др.

Как представляется, окончательное решение обозначенной проблемы применения ст. 274[1] УК РФ возможно только путем корректировки содержания отдельных пунктов постановления Пленума Верховного Суда РФ от 15 декабря 2022 г. № 37.

---

[1] См.: *Русскевич Е. А., Чекунов И. Г.* Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Уголовное право. 2022. № 5. С. 32.

[2] См.: Приговор Бежицкого районного суда г. Брянска от 5 авг. 2022 г. по делу № 1-240/2022 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: http://sudact.ru (дата обращения: 10.12.2022).

[3] См.: Приговор Октябрьского районного суда г. Владимира от 21 нояб. 2022 г. по делу № 1-351/2022 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: http://sudact.ru (дата обращения: 03.03.2023).

[4] См.: Приговор Ленинского районного суда г. Владивостока от 7 окт. 2020 г. по делу № 1-366/2020 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: http://sudact.ru (дата обращения: 03.03.2023).

Р. Р. Гайфутдинов полагает, что вредоносное воздействие на информацию не может служить критерием для признания факта причинения вреда КИИ[1]. Такой подход представляется дискуссионным ввиду своей алогичности. Получается, что законодатель в сравнении с простыми информационными ресурсами (ст. 272 УК РФ) объекты критического значения поставил под уголовно-правовую охрану лишь при условии наступления дополнительных общественно опасных последствий. Здравый смысл, равно как и системный анализ отечественного уголовного законодательства, свидетельствуют об обратном — повышение значимости объекта посягательства влечет за собой «упрощение» основания ответственности (исключение последствий, обязательного способа, специальных целей и (или) мотивов и т. п.). Это можно проследить хотя бы в известном соотношении ст. 105 и ст. 317 УК РФ.

Таким образом, в определении вреда, причиненного КИИ России, мы в большей мере склонны поддержать ранее приведенную позицию Е. А. Русскевича и И. Г. Чекунова.

Вопрос о возможности признания деяния, предусмотренного ч. 2 ст. 274[1] УК РФ, малозначительным имеет действительно острый характер. Полагаем, его следует поставить в отношении лиц, которые могут совершить неправомерный доступ к информационным объектам особой важности из соображений их проверки на предмет защищенности от взлома. Понятно, что успешная компьютерная атака на объект КИИ автоматически влечет за собой нарушение безопасности обрабатываемой таким объектом информации (только на том основании, что доступ к защищенной информации получило третье лицо). Вместе с тем «белый хакер» может сообщить о взломе владельцу, указать на ошибки и недочеты в архитектуре безопасности объекта КИИ.

В тех случаях, когда лицо, преодолев защиту объекта КИИ, по независящим от себя обстоятельствам не причинило вред, содеянное следует квалифицировать как покушение на преступление — по ч. 3 ст. 30, ч. 2 ст. 274[1] УК РФ. Важно также

---

[1] См.: *Гайфутдинов Р. Р.* Квалификация преступлений против безопасности компьютерной информации : монограф. … С. 106.

отметить, что применительно к исследуемому преступлению может быть поставлен вопрос о разделении юридического и фактического момента окончания. Так, например, лицо может на протяжении сравнительно длительного периода времени подключаться к объекту критической инфраструктуры и копировать данные. В очередной раз осуществления посягательства действия виновного могут быть прерваны сотрудниками службы безопасности. Незавершенность деяния в последнем случае не может служить поводом для квалификации содеянного как неоконченного преступления. Полагаем, что в этих условиях, состав юридически был окончен уже при первом неправомерном доступе и копировании данных.

Объективная сторона преступления, предусмотренного ч. 3 ст. 274^1 УК РФ, выражается в нарушении специальных правил эксплуатации оборудования и (или) сетей, а также правил доступа к ним.

В отечественной доктрине уголовного права ключевым и наиболее сложным вопросом в понимании данного вида неправомерного воздействия на объекты КИИ было толкование содержания соответствующих правил. В этом смысле следует позитивно оценить разъяснения Пленума Верховного Суда РФ, который в постановлении от 15 декабря 2022 г. № 37, по большому счету, поставил в этой дискуссии точку. Согласно правовой позиции Пленума к таким правилам могут относиться «как установленные нормативными актами требования, так и регулирование, вытекающее из предписаний локальных актов конкретных учреждений и организаций, правила, установленные производителем компьютерного оборудования, то есть содержащихся в соответствующей технической документации» (п. 12 Постановления № 37/2022).

В некотором смысле остался невыясненным вопрос о возможности отнесения к таким правилам требований технической документации, которые устанавливаются производителями оборудования. Как представляется, нет существенных аргументов в пользу того, чтобы не признавать такие технические предписания правилами по смыслу ст. 274^1 УК РФ.

При применении ч. 3 ст. 274[1] УК РФ органы обвинения не могут ссылаться на общее нарушение «установленного порядка». Как справедливо обосновывает Н. И. Пикуров, «при применении подобных норм требуется точное указание пунктов нарушенных правил»[1].

К преступным действиям (по смыслу ч. 3 ст. 274[1] УК РФ), к примеру, можно отнести: нарушение запрета на подключение служебного оборудования к сети «Интернет»; предоставление посторонним лицам доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации; использование нелицензионных программ; несанкционированную модификацию программного обеспечения; отключение средств противовирусной защиты; подключение постороннего оборудования и др.

Приведем пример из судебной практики.

Согласно приговору Благовещенского городского суда Амурской области от 26 июня 2020 г. по делу № 1-536/2020 К. был осужден по ч. 4 ст. 274[1] УК РФ за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре России, с использованием своего служебного положения. Суд установил, что К., нарушив правила эксплуатации информационных систем, информационно-телекоммуникационных систем, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре России, осуществил копирование электронных сведений, содержащих подробные данные о топологии сети Амурского филиала ПАО «Ростелеком», и передал их постороннему лицу, не имеющему допуска к указанным сведениям[2].

Преступление, предусмотренное ч. 3 ст. 274[1] УК РФ, может быть совершено и путем бездействия (например, виновный не выполняет обязательные процедуры периодической смены идентификаторов доступа либо резервного копирования

---

[1] *Пикуров Н. И.* Квалификация преступлений с бланкетными признаками состава : монография. М., 2009. С. 138.

[2] URL: www.судебныерешения.рф (дата обращения: 14.12.2022).

данных и т. п.). Надо признать, что в доступной для ознакомления судебной практике примеры совершения исследуемого преступления путем бездействия выявлены не были.

Уголовная ответственность по ч. 2 ст. 274[1] УК РФ и ч. 3 ст. 274[1] УК РФ может наступить только при условии, что наступившие последствия в виде причинения вреда значимым объектам КИИ России находятся в причинной связи с неправомерным доступом и допущенным нарушением правил соответственно. Установление причинной связи представляет непростую задачу при квалификации преступлений. По уголовным делам о преступлениях в сфере компьютерной информации она существенным образом осложняется их спецификой, поскольку непосредственное восприятие конкретных обстоятельств содеянного является невозможным по причине их виртуальной природы, а сами последствия зачастую являются результатом сложного взаимодействия целого ряда причин и условий.

Если причинная связь носила случайный характер, лицо не может подлежать ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Если вред КИИ России явился результатом действий (бездействия) нескольких лиц, то эти лица могут быть привлечены к ответственности по различным частям ст. 274[1] УК РФ. Так, например, прерывание функционирования значимого объекта критической информационной инфраструктуры может быть вызвано совершением компьютерной атаки, которая в свою очередь оказалась успешной только по причине безответственного поведения работника субъекта критической информационной инфраструктуры (совершившего, например, в нарушение запрета подключение служебного оборудования к сети «Интернет»). Здесь, на наш взгляд, наступление одних и тех же последствий находится в непосредственной причинной связи как с действиями хакера, квалифицировать которые следует по ч. 2 ст. 274[1] УК РФ, так и с нарушением правил работником, которое подлежит оценке по ч. 3 ст. 274[1] УК РФ.

Равным образом, если нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к КИИ России, были нарушены несколькими злоумышленниками (двумя или более лицами), каждый из которых обладал признаками субъекта преступления, предусмотренного ч. 3 или ч. 4 ст. 274[1] УК РФ, то содеянное каждым из них повлечет уголовную ответственность по данной статье. При этом важно учесть следующее условие – допущенные ими нарушения специальных правил должны были находиться в причинной связи с наступившими преступными последствиями.

Законодатель дифференцировал ответственность за неправомерное воздействие на КИИ России в ч. 5 ст. 274[1] УК РФ в зависимости от наступления «тяжких последствий». Редакция данной части вызывает вопросы. Если в других составах преступлений в сфере компьютерной информации обычно указывается на наступление таких последствий либо *о создании угрозы их наступления* (выделено мной — *И. М.*), то в ч. 5 ст. 274[1] УК РФ законодатель закрепляет только «наступление тяжких последствий». «Видеть здесь какой-то замысел законодателя, на наш взгляд, было бы наивным, как и было бы неискренним попытаться объяснить или оправдать такое решение. Полагаем, что при разработке исследуемой нормы нарушение системности законодателем было допущено по ошибке»[1]. Аналогичную точку зрения о редакции ч. 5 ст. 274[1] УК РФ высказывают С. Д. Бражник и А. А. Чавгун[2].

Рассуждая о тяжких последствиях, Л. Л. Кругликов пишет, что частота использования квалифицирующего признака «тяжкие последствия» в уголовном

---

[1] *Малыгин И. И.* О совершенствовании уголовного законодательства об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Российской правовой академии. 2021. №3. С. 118 – 121.

[2] См.: *Бражник С. Д., Чавгун А. А.* Неправомерное воздействие на критическую информационную инфраструктуру России: дискуссионные вопросы регламентации и толкования квалифицирующего признака, характеризующего тяжкие последствия // Наука, образование, общество: тенденции и перспективы развития : сборник. 2019. С. 141.

законе устойчиво занимает второе место после группового характера преступления. При этом содержание этого признака во всех главах существенно разнится, что, по мнению автора, обязывает толковать «тяжкие последствия» применительно к отдельным главам Особенной части УК РФ[1].

С данным утверждением нельзя не согласиться. Действительно, вряд ли толкование такого оценочного признака, как «тяжкие последствия», может иметь абсолютно универсальный характер для всего уголовного закона. Вместе с тем стоит указать, что в известном смысле такие последствия должны пониматься если и не тождественно, то хотя бы достаточно однородно.

Пленум Верховного Суда РФ разъяснил, что «к тяжким последствиям применительно к компьютерным преступлениям следует относить длительную приостановку 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.» (Постановление № 37/2022).

Полагаем, Пленум Верховного Суда РФ совершенно справедливо оставляет указанный список открытым, поскольку очевидно, что указанные виды тяжкого вреда далеко не исчерпывают явления. С другой стороны, вызывает серьезные возражения указание на то, что как тяжкие необходимо оценивать последствия, заключающиеся в получении виновным доступа к конфиденциальным данным. В этом смысле значительное количество посягательств на компьютерные данные априорно будет сопряжено с тяжкими последствиями (любой взлом электронной почты либо аккаунта в социальной сети). С нашей точки зрения, в данной части правовая позиция Пленума требует детального анализа и обсуждения. Другое дело, когда в качестве тяжкого последствия называется размещение соответствующих сведений в открытом доступе. Однако и в этом случае решение может быть не столь однозначным. Возможно, следует говорить не о любых

[1] См. об этом: *Кругликов Л. Л.* Тяжкие последствия в уголовном праве: объективные и субъективные признаки // Уголовное право. 2010. № 5. С. 38.

конфиденциальных данных, а лишь о тех, которые создают угрозу, например, для государственной и общественной безопасности.

Кроме того, нельзя не заметить, что определение тяжких последствий осуществляется Пленумом также с использованием оценочных признаков — длительная приостановка либо нарушение работы организации. Понятно, что вопрос о длительности в свое время станет предметом самых бескомпромиссных дискуссий при применении ч. 5 ст. 274^1 УК РФ.

Полагаем, что применительно к исследуемому составу преступления признак «тяжкие последствия» может иметь следующее содержание:

1) гибель людей;

2) массовое отравление;

3) причинение значительного экологического вреда;

4) дезорганизация работы транспорта, объектов транспортной инфраструктуры с созданием угрозы для жизни и здоровья граждан;

5) утрата сведений, составляющих государственную тайну;

6) нарушение работы предприятия с созданием угрозы для жизни и здоровья человека либо с причинением особо крупного ущерба и др.

Приведенный список, конечно же, может быть дополнен. Жизнь гораздо богаче самых смелых представлений о ней. Вместе с тем видится, что указанные вредные последствия выступают безусловным основанием, чтобы квалифицировать неправомерное воздействие на КИИ России.

Исследование объективных признаков неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации позволяет сделать следующие выводы.

1. Объектом преступления, предусмотренного ст. 274^1 УК РФ, являются общественные отношения, связанные с построением и развитием в России информационного общества, цифровой экономики и электронного правительства.

2. Предмет преступления, предусмотренного ст. 274^1 УК РФ, представляет собой значимый объект критической информационной инфраструктуры

Российской Федерации (независимо от категории значимости), характеризующийся двумя критериями:

а) *критерием значимости*, то есть социальной, политической, экономической, экологической или оборонной важности;

б) *реестровым критерием*, связанным с включением объекта в Реестр значимых объектов КИИ.

Признание соответствующего объекта информационной инфраструктуры предметом преступления, предусмотренного ст. 274[1] УК РФ, допустимо только при наличии обоих указанных критериев.

3. Перечень отраслей, в которых могут быть выделены объекты КИИ, искусственно ограничен. 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 полагаем, что п. 8 ст. 2 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» необходимо дополнить.

4. Применительно к ч. 1 ст. 274[1] УК РФ нельзя оценивать как использование вредоносной компьютерной программы (информации) 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.

5. 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.

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

7. По смыслу ч. 5 ст. 274[1] УК РФ под «тяжкими последствиями» следует понимать:

а) гибель людей;

б) массовое отравление;

в) причинение значительного экологического вреда;

г) дезорганизацию работы транспорта, объектов транспортной инфраструктуры с созданием угрозы для жизни и здоровья граждан;

д) утрату сведений, составляющих государственную тайну;

е) нарушение работы предприятия с созданием угрозы для жизни и здоровья человека либо с причинением особо крупного ущерба и др.

§ 2. Уголовно-правовая характеристика субъективных признаков неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Субъект неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Содержание признаков субъекта неправомерного воздействия на КИИ России, пожалуй, нельзя отнести к числу проблемных вопросов для правоприменительной практики или вызывающих значительные дискуссии в отечественной теории.

Изучение имеющихся публикаций позволяет сделать вывод, что широко обсуждаемыми являются следующие аспекты характеристики субъекта исследуемого преступления:

1) установление возраста уголовной ответственности за посягательства на информационные системы особой важности с 16 лет и обоснованность такого подхода[1];

2) определение признаков субъекта нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, информационных системах, информационно-телекоммуникационных сетях, автоматизированных системах управления, сетях электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, а также правил доступа к указанным информационным системам управления, сетям автоматизированных систем управления, сетям электросвязи (ч. 3 ст. 274[1] УК РФ);

---

[1] *Малыгин И. И.* О совершенствовании уголовного законодательства об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Российской правовой академии. 2021. №3. С. 118 – 121.

3) определение признаков специального субъекта — лицо, совершающее неправомерное воздействие на КИИ России с использованием своего служебного положения (ч. 4 ст. 274[1] УК РФ).

Можно с уверенностью утверждать, что проблема понижения возраста уголовной ответственности за отдельные преступления обсуждается в отечественной доктрине уголовного права непрерывно. К этому уголовно-политическому инструменту, как правило, прибегают, ссылаясь на распространенность конкретных форм общественно опасного поведения среди несовершеннолетних, а также на высокий уровень развитости современной молодежи в IT-сфере. Действительно, сложно оспорить тот факт, что современные дети быстрее и эффективнее осваивают цифровые технологии. Поколение отцов делает это либо из профессиональной, либо иной необходимости, с вполне явственным скепсисом к легковесности виртуального мира. В то же время миллениалы относятся к киберпространству как к неотъемлемой части своей жизни, аккаунты в социальных сетях выступают цифровым продолжением себя. Отсюда и отчетливо просматривается тенденция гораздо более чуткого отношения молодого поколения к своим цифровым правам и острого реагирования на посягательства в отношении них.

В 2018 году ПАО «Сбербанк России» представил весьма интересные результаты исследования: «около 10 % киберпреступников имеют достаточно юный возраст (14–15 лет). При этом 85–90 % киберпреступников в мире — это молодые люди не старше 20 лет»[1].

Еще в начале 2000-х годов идея понизить возраст привлечения к уголовной ответственности за компьютерные преступления (с 16 до 14 лет) была высказана А. Ж. Кабановой[2].

---

[1] В Сбербанке рассчитали долю совершенных детьми киберпреступлений [Электронный ресурс]. URL: https://www.rbc.ru/society/04/07/2018/5b3ceb009a7947b19e91997e (дата обращения: 15.05.2022).

[2] См.: *Кабанова А. Ж.* Преступления в сфере компьютерной информации: уголовно-правовые и криминологические аспекты : автореф. дис. … канд. юрид. наук : 12.00.08. Ростов н/Д, 2004. С. 4.

Оценивая этот же вопрос о понижении возраста ответственности К. Н. Евдокимов, в свою очередь, полагает, что такое решение имеет под собой основания, однако лишь за преступления в сфере компьютерной информации при отягчающих обстоятельствах[1].

Полагаем, что такая идея требует серьезной эмпирической основы и тщательной теоретической проработки. Как показало проведенное исследование (выборка из 412 приговоров), доля несовершеннолетних, которые были осуждены за преступления в сфере компьютерной информации, составляет всего 8,7 %. По немногочисленным делам об исследуемом преступлении таких лиц выявлено не было вовсе. Мысль о том, что к совершению подобных деяний почти не причастны подростки также была обозначена некоторыми респондентами в ходе проводимых в процессе подготовки исследования интервью.

Полагаем, что подлинно научный ответ на вопрос о снижении возраста ответственности за компьютерные преступления в целом и неправомерное воздействие на КИИ России 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 мы имеем недостаточный опыт, и подобное решение о понижении возраста ответственности за преступления в сфере компьютерной информации видится преждевременным.

Хотя общепринятым постулатом уголовно-правовой теории является идея о том, что субъект преступления, связанного с нарушением специальных правил,

---

[1] См.: *Евдокимов К. Н.* Актуальные вопросы противодействия компьютерной преступности в Российской Федерации (криминологическое исследование) // Российский следователь. 2018. № 10. С. 61.

ввиду специфики осуществляемой им роли в механизме соответствующих правоотношений, всегда является специальным[1], в отечественной теории уголовного права нет однозначного подхода к тому, как понимаются признаки субъекта нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации.

Одни авторы полагают, что субъект преступления, предусмотренного ч. 3 ст. 274[1] УК РФ, общий — физическое вменяемое лицо, достигшее 16-летнего возраста[2].

В свою очередь А. Н. Попов формулирует вывод об альтернативном характере субъекта исследуемого преступления следующим образом: «Субъект может быть как общим, так и специальным. … если на лице лежала обязанность по соблюдению специальных правил, то субъект преступления специальный. Если на лице не лежала обязанность по соблюдению специальных правил, то субъект преступления признается общим»[3].

Е. А. Русскевич отстаивает позицию о том, что субъект преступления, предусмотренного ч. 3 ст. 274[1] УК РФ, только специальный – «лицо, на которое в силу закона, иного нормативного акта либо характера выполняемой профессиональной, трудовой или иной деятельности возложена обязанность по соблюдению соответствующих правил эксплуатации или доступа»[4].

Подобную точку зрения обосновывает и Ю. В. Трунцевский, отмечая, что «субъект исследуемого преступления — специальный: это вменяемое лицо, достигшее возраста 16 лет, имеющее доступ к критической информационной инфраструктуре Российской Федерации либо к относящимся к ней объектам

---

[1] См., например: *Кудрявцев В. Н.* Общая теория квалификации преступлений. М., 2007. С. 162–163 ; *Пудовочкин Ю. Е.* Учение о составе преступления. М., 2009. С. 223.

[2] См.: Уголовное право России. Общая и Особенная части : учебник / Под ред. д-ра юрид. наук, проф. В. К. Дуюнова. … С. 665.

[3] *Попов А. Н.* Преступления в сфере компьютерной информации : учеб. пособие. СПб., 2018. С. 49.

[4] См.: *Русскевич Е. А.* Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. … д-ра юрид. наук. М., 2020. С. 323.

в силу выполнения служебных обязанностей по исполнению установленных правил эксплуатации и доступа к критической информационной инфраструктуре Российской Федерации»[1].

Полагаем, что именно последний подход к юридической характеристике субъекта нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 3 ст. 274[1] УК РФ), может быть признан наиболее обоснованным. Как справедливо пишет по данному поводу Н. И. Пикуров: «… признаки специального субъекта тесно связаны с другими признаками состава преступления, в том числе характеризующими объективную сторону… так как преступление есть неразрывное единство деяния лица (действия, бездействия) и того, кто его совершает (субъекта преступления)»[2].

В примерах судебно-следственной практики субъекты нарушения правил по ч. 3 ст. 274[1] УК РФ также обладают дополнительными признаками (выступают руководителями различного уровня или работниками соответствующих организаций). Так, в приговоре Благовещенского городского суда Амурской области от 26 июня 2020 г. по делу № 1-536/2020 суд, осуждая К. по ч. 4 ст. 274[1] УК РФ, подробно указал, что он «допустил нарушение правил эксплуатации средств хранения, обработки и передачи охраняемой компьютерной информации… в нарушение пунктов трудового договора и служебных инструкций, предусмотренных: п. 3.5 Порядка предоставления прав доступа, Политики управления доступом к информационным активам в Макрорегиональном филиале "Дальний Восток ОАО Ростелеком", утвержденной приказом ПАО "Ростелеком"; п. 3.2 Ограничений при работе с паролями/PIN-кодами; п. 4.4 документа об ответственности пользователей автоматизированного

---

[1] *Трунцевский Ю. В.* Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 105.

[2] *Пикуров Н. И.* Квалификация преступлений с бланкетными признаками состава : монография. М., 2009. С. 210.

рабочего места, Политики использования паролей в Макрорегиональном филиале "Дальний Восток" ОАО "Ростелеком", утвержденной приказом ПАО "Ростелеком"; п. 5 Порядка обращения с информацией, составляющей коммерческую тайну; п. 6 документа об охране конфиденциальности информации в рамках трудовых отношений, Положения о режиме коммерческой тайны в ОАО "Ростелеком"; п. 3 Порядка обращения с информацией, составляющей коммерческую тайну; п. 5 Порядка ознакомления работников Общества с информацией, составляющей коммерческую тайну; п. 6 Порядка передачи и предоставления информации, составляющей коммерческую тайну, Процедуры по обращению с информацией, составляющей коммерческую тайну; п. 2.2 Правил работы и ограничения при доступе в Интернет; п. 3 Обязанностей должностных лиц и служб Положения об использовании ресурсов сети "Интернет" в Макрорегиональном филиале "Дальний Восток" ОАО "Ростелеком"».

И наконец, обратим внимание, что, разъясняя обязательное условие наступления ответственности по ст. 274 УК РФ, Пленум Верховного Суда РФ указал, что соответствующие правила должны быть доведены до работника при подписании трудового договора, специального соглашения об информационной политике компании или иного акта (п. 12 Постановления № 37/2022). Принимая во внимание объективную близость нормативных конструкций, справедливым видится распространение данного разъяснения и на положения ч. 3 ст. 274^1 УК РФ. Таким образом, это еще раз подтверждает тезис о специальном субъекте данного состава преступления.

Отдельного комментария заслуживает вопрос о том, возможно ли признавать субъектом преступления, предусмотренного ч. 3 ст. 274^1 УК РФ, лицо, которое не было оформлено в установленном порядке на должность, однако постоянно либо временно фактически исполняет обязанности в организации, связанные с необходимостью соблюдения правил эксплуатации и доступа к объектам критической информационной инфраструктуры.

Данная проблематика хорошо разработана в отечественной теории уголовного права применительно к составам преступлений, связанным

с нарушением специальных правил в целом[1]. Исходя из современной доктрины уголовного права и не вдаваясь в полемику, можно заключить, что 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[2].

Квалифицированным видом неправомерного воздействия на объекты КИИ по признакам субъекта является совершение этого преступления лицом с использованием своего служебного положения. Что следует понимать под такой категорией лиц закреплено в в п. 29 постановления Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 (ред. от 15 декабря 2022 г.) «О судебной практике по делам о мошенничестве, присвоении и растрате»[3]. Смысл разъяснений заключается в том, чтобы признавать такими субъектами должностных лиц и лиц, наделенных управленческими функциями в коммерческих и иных организациях.

Однако по другой категории уголовных дел в другом, более раннем своем постановлении Пленум Верховного Суда РФ указал, что такими субъектами можно «признавать и иных лиц, не обладающих управленческими компетенциями, — это работники, выполнение трудовых функций которых связано с доступом к определенным предметам, оборудованию и т. д.»[4].

Обстоятельно вопрос о толковании данного признака применительно к составам компьютерных преступлений раскрыл в своей работе Е. А. Русскевич. Автор делает общий вывод, что «проблема более строгой ответственности лиц,

---

[1] См., например: *Мирошниченко Н. В*. Теоретические основы уголовной ответственности за преступления, связанные с нарушением специальных функций. М., 2014; Пикуров Н. И. Квалификация преступлений с бланкетными признаками состава: монограф. М., 2009 и др.

[2] Данный вывод нашел свою поддержку у 79 % опрошенных респондентов (см. приложение Б, с. 189–193).

[3] Официальный сайт Верховного Суда РФ. URL: www.vsrf.ru (дата обращения: 10.03.2023).

[4] Постановление Пленума Верховного Суда Рос Федерации от 15 июня 2006 г. № 14 «О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами» : ред. от 16 мая 2017 г. [Электронный ресурс] // Официальный сайт Верховного Суда РФ. URL: www.vsrf.ru (дата обращения: 10.03.2023).

обязанных в силу выполняемых ими трудовых функций соблюдать и (или) обеспечивать информационную безопасность организации, требует отказа от классического (ограничительного) толкования лиц, использующих служебное положение, и отнесения к данной категории по сути любых сотрудников, которые на законных основаниях используют компьютерную информацию компании или учреждения, а также средства ее обращения (системные инженеры, программисты, менеджеры, продавцы-консультанты и специалисты по обслуживанию клиентов, обладающие полномочиями по использованию баз данных и др.)»[1].

Поддерживая данную точку зрения в целом, необходимо сделать одно важное уточнение. Данный квалифицирующий признак распространяется на преступление, предусмотренное ч. 3 ст. 274[1] УК РФ, где, как уже было отмечено ранее, субъект и так обладает специальными признаками. Применительно к ст. 274 УК РФ такой проблемы не возникало, поскольку законодатель не дифференцирует там ответственность по исследуемому основанию (почему это было реализовано в ст. 274[1] — остается загадкой). Так или иначе, применительно к составу нарушения правил эксплуатации и доступа рекомендации Е. А. Русскевича, что называется, не работают. В связи с этим считаем, что толкование данного квалифицирующего признака применительно к ч. 1 и ч. 2 ст. 274[1] УК РФ должно быть расширительным — в качестве такого лица может выступать любое лицо, которое обязано в силу выполняемых им профессиональных функций соблюдать и (или) обеспечивать информационную безопасность объектов КИИ России. Однако в отношении деяния, описанного в ч. 3 ст. 274[1] УК РФ, его толкование должно быть ограничительным — должностные лица, обладающие признаками, предусмотренными п. 1 примечания к ст. 285 УК РФ, государственные или муниципальные служащие, не являющиеся

[1] *Русскевич Е. А.* О квалификации преступлений в сфере компьютерной информации, совершаемых с использованием служебного положения // Российское правосудие. 2019. № 2. С. 35–41.

должностными лицами, а также иные лица, отвечающие требованиям, предусмотренным п. 1 примечания к ст. 201 УК РФ.

Субъективная сторона неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Традиционно вопросы, связанные с внутренним отношением виновного к содеянному, являются наиболее дискуссионными в доктрине уголовного права и крайне сложными на правоприменительном уровне. Исследуемые посягательства в этом отношении характеризуются еще большей противоречивостью в установлении субъективных признаков состава.

Деяние, предусмотренное ч. 1 ст. 274^1 УК РФ, может быть совершено исключительно с прямым умыслом. При этом лицо, осуществляя действия, направленные на создание вредоносных компьютерных программ, их использование либо распространение, должно осознавать их специфический функциональный ресурс — заведомую эффективность в отношении объектов КИИ.

Выяснение и обоснованность в приговоре такой осведомленности может основываться на разных объективных данных. Полагаем, что в случае с разработчиком направленность на объекты КИИ не может им не учитываться просто потому, что на определенном этапе создания требуется непосредственное подтверждение действенности имеющегося вредоносного программного обеспечения. Объективные сложности в квалификации по ч. 1 ст. 274^1 УК РФ возникают в тех случаях, когда в разработке участвовало сразу несколько программистов, при этом каждый из них выполнял лишь часть работ, не имея полного представления об итоговом результате. С точки зрения учения о вине привлекать таких субъектов к уголовной ответственности именно за создание вредоносов против критической информационной инфраструктуры будет невозможно.

При использовании субъективная направленность именно на критически важные объекты также без труда может быть установлена из самого характера совершаемой атаки.

Гораздо сложнее дело может обстоять с квалификацией распространения, поскольку, размещая в открытом доступе вредоносное программное обеспечение, лицо может не обладать полными знаниями относительно функционала конкретной программы. Полагаем, что здесь весьма важно получить иные достоверные сведения о такой осведомленности, например, в ходе проведения оперативного эксперимента либо иных мероприятий.

При неправомерном доступе (ч. 2 ст. 274[1] УК РФ) умысел может быть как прямым, так и косвенным. Согласно ранее обоснованному тезису применительно к неправомерному доступу «по смыслу ст. 272 УК РФ такое посягательство также характеризуется неосторожностью»[1]. Однако согласиться с данной точкой зрения нельзя. Неправомерный доступ как деяние предполагает известную направленность — стремление к получению возможности ознакомления, копирования, модификации, блокирования и уничтожения защищенной компьютерной информации. Если лицо воспользовалось компьютером, на котором оказался открыт аккаунт социальной сети другого пользователя (случайно, по стечению обстоятельств), это не означает, что последующие манипуляции с этим аккаунтом (изменение сетевых идентификаторов, копирование переписки, размещение изображений или оставление комментариев и т. п.) содержат признаки совершенного по неосторожности неправомерного доступа к компьютерной информации. И в этом случае неправомерный доступ к компьютерной информации носит умышленный характер, с той лишь разницей, что виновному по причине забывчивости владельца аккаунта не пришлось преодолевать средства программно-технической защиты.

---

[1] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] // Документы – Генеральная прокуратура Российской Федерации : сайт. URL: www.epp.genproc.ru, 14.04.2014 (дата обращения: 16.01.2023).

Здесь возникает вопрос, на который довольно сложно дать определенный ответ с точки зрения действующей редакции исследуемой нормы. Вопрос этот связан с квалификацией действий лица, которое в силу стечения обстоятельств по ошибке совершает атаку на критически важный объект, хотя изначальный замысел был связан с вмешательством в работу, например, небольшой компании. Этот вопрос будет рассмотрен нами немного позднее в рамках данной части работы.

Субъективная сторона преступления, предусмотренного ч. 3 ст. 274[1] УК РФ, характеризуется двумя формами вины — умыслом и неосторожностью[1].

Верно указывает Н. Ш. Козаев, что «неуказание на форму вины в составе нарушения правил эксплуатации средств хранения, обработки или передачи компьютерных данных (автор формулирует данный вывод применительно к ст. 274 УК РФ — *И. М.*) является упущением законодателя, поскольку сама конструкция состава логически требует признания возможности совершения деяния по неосторожности, но ч. 2 ст. 24 УК РФ позволяет признавать преступление совершенным по неосторожности, только если это предусмотрено соответствующей статьей Особенной части УК РФ»[2].

Следует заметить, что наличие подобных норм, равно устанавливающих ответственность за умышленное и неосторожное поведение, вряд ли может восприниматься как положительное явление в рамках механизма уголовно-правовой охраны. Слишком несопоставимым может быть поведение субъектов. Так, в одном случае лицо, допущенное к работе в системе, целенаправленно заражает ее вредоносной программой и осуществляет манипуляции с содержанием и функционалом системы. В другом же случае, например, бухгалтер уговаривает системного администратора снять некоторые ограничения на использование служебного оборудования и происходит то же заражение, но по причине использования личной электронной почты работника.

---

[1] См.: Уголовно-юрисдикционная деятельность в условиях цифровизации : монограф. / Н. А. Голованова, А. А. Гравина, О. А. Зайцев и др. М. : ИЗиСП, КОНТРАКТ, 2019. 212 с.

[2] *Козаев Н. Ш.* Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства) : монограф. М., 2015. С. 172.

Одним из значимых вопросов квалификации неправомерного воздействия на объекты критической информационной инфраструктуры Российской Федерации является проблема отражения свойств предмета преступного посягательства в сознании виновного. Иными словами, предполагает ли ст. 274[1] УК РФ установление осведомленности виновного о принадлежности компьютерной информации именно к объектам критической информационной инфраструктуры Российской Федерации? Если исходить из известного тезиса, что все юридически значимые обстоятельства совершения преступления (конструктивные, квалифицирующие и привилегирующие признаки состава преступления) должны получить отражение в сознании виновного, то ответ на поставленный вопрос должен быть утвердительным.

Р. Р. Гайфутдинов пишет по данному поводу: «… деятель должен осознавать характер своего деяния: что доступ осуществляется неправомерно, то есть понимать то, что им нарушаются определенные правомерные способы доступа к охраняемой законом компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации… исполнитель преступления должен осознавать, что компьютерная информация охраняется законом…, осознавать, что компьютерная информация содержится в критической информационной инфраструктуре Российской Федерации. Иными словами, осознавать наличие всех признаков предмета преступления»[1].

Изучение имеющейся правоприменительной практики показывает, что органы предварительного расследования и суды при описании признаков субъективной стороны неправомерного воздействия на объекты критической информационной инфраструктуры Российской Федерации напрямую указывают, что лицо осознавало специфические признаки предмета посягательства[2]. Однако, здесь следует сделать важную оговорку — соответствующие приговоры

---

[1] *Гайфутдинов Р. Р.* Квалификация преступлений против безопасности компьютерной информации : монограф. … С. 117–118.

[2] См.: Приговор Благовещенского городского суда Амурской области от 26 июня 2020 г. по делу № 1-536/2020 ; приговор Абаканского городского суда Республики Хакасия от 29 июля 2020 г. по делу № 1-805/2020 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: www.sudact.ru (дата обращения: 20.12.2022).

выносились в отношении работников организаций, информационные системы которых оказались скомпрометированы. Вывод об осведомленности закономерно вытекал из того, что лицо, занимая соответствующую должность в организации и используя служебные информационные ресурсы, было заранее в установленном порядке проинформировано, что они отнесены к объектам критической информационной инфраструктуры Российской Федерации.

В отношении же остальных лиц такой вывод однозначно сделать нельзя. Как известно, относимость того или иного информационного ресурса к критическому определяется посредством его включения в Реестр значимых объектов критической информационной инфраструктуры (ст. 8 Закона о безопасности КИИ России), содержание которого, в отличие от того же перечня наркотических средств, имеет закрытый характер.

Вместе с тем при неправомерном доступе (ч. 2 ст. 274^1 УК РФ) умысел может быть как прямым (конкретизированным), так и косвенным (неконкретизированным). Осуществляя посягательство на информационные системы, функционирующие, например, в энергетическом комплексе Российской Федерации, лицо осознает вероятность включения соответствующих систем в Реестр значимых объектов критической информационной инфраструктуры. Осознание специфических признаков предмета посягательства здесь основывается не на изучении положений Реестра (что невозможно), а на понимании описанных в Законе о безопасности КИИ России сущностных признаков соответствующих объектов, а именно — их принадлежности к информационным системам государственных органов, оборонной промышленности, области здравоохранения, транспорта, связи, кредитно-финансовой сфере, энергетике и т. д.

Подобный подход к пониманию содержания умысла неправомерного воздействия на объекты критической информационной инфраструктуры Российской Федерации нашел свое отражение и на уровне правоприменительной практики. Так, соглашаясь с квалификацией действий виновных по ч. 4 ст. 274^1 УК РФ, суд сослался на то, что модификация и блокирование охраняемой

компьютерной информации были осуществлены в информационных системах и информационно-телекоммуникационных сетях, функционирующих в субъекте оборонной промышленности, о чем виновные были осведомлены[1].

Проблема установления признаков субъективной стороны преступления, предусмотренного ст. 274[1] УК РФ, предстает совершенно в ином значении, когда лицо осуществляет компьютерную атаку с конкретным умыслом на информационные ресурсы субъекта, не имеющего отношения к КИИ России, однако в результате этого информационным системам особой важности также причиняется вред. В отечественной правоприменительной практике подобная ситуация не возникала, но такие примеры можно легко обнаружить в зарубежной практике.

Так, 10 сентября 2020 г. компьютерная атака привела к блокированию компьютерных систем одной из клиник Дюссельдорфа в Германии. В течение недели работа медучреждения была нарушена — злоумышленники зашифровали данные на нескольких серверах, потребовав выкуп за снятие блокировки. Из-за масштабного сбоя сотрудники больницы не могли оказывать медицинскую помощь. Один из пациентов больницы, находясь в тяжелом состоянии, умер по дороге в соседний город. Анализ инцидента позволил полиции сделать вывод, что целью преступников был Университет им. Генриха Гейне. Компьютерные системы больницы оказались заблокированы только потому, что медицинская организация использовала с университетом одни и те же сервера. Полиции удалось связаться с вымогателями и объяснить им, что атака затронула клинику, подвергнув опасности жизни людей. После этого хакеры предоставили ключ для расшифровки данных[2].

Полагаем, что в подобной ситуации, если виновные, опираясь на объективные факторы, действительно по ошибке атаковали объект КИИ России,

---

[1] Приговор Первомайского районного суда г. Владивостока от 25 сент. 2019 г. по делу № 1-376/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: www.sudact.ru (дата обращения: 20.12.2022).

[2] *Черненко Е., Цуканов П.* Хакеры смерти. Россию обвиняют в очередной кибератаке, на сей раз – с летальным исходом [Электронный ресурс] // Газета «Коммерсантъ». URL: www.kommersant.ru (дата публикации: 28.09.2020 ; дата обращения: 19.12.2020).

квалифицировать содеянное по ст. 274[1] УК РФ нельзя. Здесь необходимо применять общую норму об ответственности за неправомерный доступ к компьютерной информации (ст. 272 УК РФ). При этом, учитывая, что доступ был осуществлен к объектам КИИ России, оценивать содеянное нужно как повлекшее наступление тяжких последствий, то есть по ч. 4 ст. 272 УК РФ.

Исследование субъективных признаков неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации позволяет сделать следующие выводы.

1. Подлинно научный ответ на вопрос об изменении возрастных границ уголовной ответственности в сторону снижения за преступления в сфере компьютерной информации в целом и неправомерное воздействие на КИИ России 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, и решение о снижении возраста уголовной ответственности за преступления в сфере компьютерной информации видится преждевременным.

2. 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.

3. Толкование квалифицирующего признака «служебное положение лица» при неправомерном воздействии на КИИ России носит двойственный характер:

а) применительно к ч. 1 и ч. 2 ст. 274[1] УК РФ оно должно быть расширительным — в качестве такого лица может выступать любое лицо, которое

обязано в силу выполняемых им профессиональных функций соблюдать и (или) обеспечивать информационную безопасность объектов КИИ России;

б) в отношении деяния, описанного в 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.

4. 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 следует как повлекшее наступление тяжких последствий, то есть по ч. 4 ст. 272 УК РФ.

Глава 3. Вопросы совершенствования уголовного законодательства и проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

При осуществлении юридического анализа преступления, предусмотренного ст. 274[1] УК РФ, многие проблемы квалификации исследуемого преступления уже были выделены и рассмотрены. Вместе с тем остались незатронутыми многие вопросы юридической оценки неправомерного воздействия на КИИ России, возникающие, что называется, «на стыке» с основными институтами отечественного уголовного права (соучастие, неоконченное преступление, множественность). Данному блоку проблем и будет посвящен первый параграф настоящей главы.

Кроме того, традиционным в отечественной доктрине уголовного права является самостоятельное рассмотрение возможных перспектив модернизации отечественного уголовного закона по исследуемой проблематике. Не будет исключением и настоящая работа. Здесь стоит отметить, что значимость и актуальность разработки вопросов совершенствования уголовно-правовой нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации объясняется и тем обстоятельством, что в настоящее время уже подготовлен и проходит обсуждение законопроект о внесении изменений в ст. 274[1] УК РФ.

Содержание данной главы во многом направлено в будущее и имеет своей целью смоделировать наиболее приемлемые подходы на уровне правоприменения, а также указать на перспективное (по мнению автора, необходимое) развитие отечественного уголовного законодательства. Справедливость сформулированных выводов, как обычно, будет верифицирована временем.

§ 1. Проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

Вопросы практической реализации уголовной ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации нельзя отнести к числу хорошо разработанных в отечественной теории уголовного права. Имеющиеся публикации преимущественно посвящены осмыслению самой криминализации посягательства на информационные объекты особой важности, а также анализу отдельных юридико-технических особенностей конструкции ст. 274[1] УК РФ[1]. Вместе с тем с момента самостоятельного определения уголовно-правовой нормы об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации прошло уже более пяти лет. Период достаточный, чтобы можно было подвести определенные итоги и сформулировать некоторые рекомендации de lege lata.

Традиционно проблемным является вопрос о квалификации соучастия в совершении неправомерного воздействия на КИИ России. Как справедливо отмечается в отечественной литературе, «компьютерная преступность характеризуется специфической архитектурой криминальных связей»[2].

---

[1] См. об этом: *Решетников А. Ю., Русскевич Е. А*. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК России) // Законы России: опыт: анализ, практика. 2018. № 2 (66). С. 51–55 ; *Степанов-Егиянц В. Г*. Критическая информационная инфраструктура России: понятие и вопросы уголовно-правовой охраны // Евразийский юридический журнал. 2019. № 2 (129). С. 265–268 ; *Кругликов Л. Л., Бражник С. Д., Пилясов И. А*. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ): некоторые проблемы определения признаков состава преступления // Журнал юридических исследований. 2019. Т. 4. № 3. С. 53–62 и др.

[2] *Дмитренко А. П., Русскевич Е. А*. О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий // Вестник Академии Генеральной прокуратуры Российской Федерации. 2017. № 5 (61). С. 18.

Принимая во внимание наличие квалифицирующих признаков в зависимости от группового способа (ч. 4 ст. 274[1] УК РФ), необходимо по возможности детально разработать проблему разграничения совершения исследуемого преступления в сложном соучастии, в составе предварительно сговорившейся группы, а также группы организованной.

Здесь наибольшую актуальность представляет уголовно-правовая оценка неправомерного доступа к компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации. Объективная сторона преступления, предусмотренного ст. 274[1] УК РФ, имеет сложный характер и заключается не только в непосредственном преодолении средств программно-технической защиты, но и в последующих действиях по копированию, уничтожению, блокированию или модификации компьютерной информации. Полагаем, что для квалификации неправомерного доступа к компьютерной информации, содержащейся в КИИ России группой лиц по предварительному сговору по ч. 4 ст. 274[1] УК РФ неважно, участвовали ли все сговорившиеся лица в проникновении либо по распределению ролей один из соучастников «взламывал» систему, а другие совершали последующие манипуляции с компьютерной информацией, что повлекло причинение вреда критической информационной инфраструктуре Российской Федерации.

Кроме того, лица, предварительно сговорившиеся на совершение неправомерного доступа, могут поочередно предпринимать попытки проникновения в защищенную информационную систему. При достижении общей преступной цели одним из них содеянное также следует квалифицировать по ч. 4 ст. 274[1] УК РФ.

Не может образовывать признаков группового совершения неправомерного доступа к КИИ участие двух лиц, при котором один из них лишь склонил другого к совершению деяния, оказал ему в той или иной форме содействие (например, профинансировал приобретение вредоносных компьютерных программ), но непосредственно не участвовал ни в попытках проникновения в систему, ни в оказании вредоносного воздействия на хранящуюся в ней компьютерную

информацию. В зависимости от фактических обстоятельств дела содеянное, на наш взгляд, следует квалифицировать как организацию, подстрекательство либо пособничество в совершении неправомерного доступа к критической информационной инфраструктуре.

Совершение посягательства на объекты КИИ в составе организованной группы может быть признано таковым лишь при наличии признаков, предусмотренных ч. 3 ст. 35 УК РФ. Признак устойчивости не может быть доказано исключительно ссылками на сложившиеся между конкретными лицами и поддерживаемыми на протяжении длительного времени отношениями. Пусть хотя бы и по поводу обмена информацией о способах и средствах совершения компьютерных преступлений. Такая хактивистская кооперация (как форма «профессионального» сотрудничества и личного общения) еще не образует устойчивости в соучастии (да и самого соучастия, по большому счету, не образует). Необходимо выявить достижение между такими лицами сговора; то, что они объединили свои усилия именно на совершение конкретных преступлений. Иначе, можно ставить вопрос о наличии в содеянном признаков сложного соучастия (например, пособничества), либо о том, что соучастия в данном случае и вовсе не было.

Важным и непростым вопросом квалификации соучастия в неправомерном воздействии на КИИ России является определение пределов вменения каждому из соучастников юридически значимых обстоятельств совместно совершенного преступления. Нельзя не отметить, что в целом подобная проблематика нашла свое обстоятельное рассмотрение в известной работе А. И. Рарога[1]. Этот вопрос может возникнуть перед судебно-следственными органами как при квалификации создания, использования и распространения вредоносных компьютерных программ, заведомо предназначенных для совершения воздействия на критическую информационную инфраструктуру Российской Федерации, так и при оценке неправомерного доступа к такой инфраструктуре. По тем или иным

[1] См.: *Рарог А. И.* Проблемы квалификации преступлений по субъективным признакам : монограф. М., 2015. 232 с.

причинам лицо может сознательно вводить в заблуждение или умалчивать о направленности соответствующих деяний на информационные объекты особого значения. При подобных обстоятельствах наблюдается ситуация, когда лицо в целом было осведомлено о факте совместного совершения компьютерного преступления, но заблуждалось о важнейших особенностях предмета посягательства. Исходя из общего принципа, согласно которому соучастнику вменяется только то, что охватывалось его умыслом, можно сделать следующий вывод: вопрос о пределах вменения при соучастии в неправомерном воздействии на КИИ России должен решаться с учетом объема вины. Заблуждение одного из соучастников относительно направленности совершаемого деяния на критическую информационную инфраструктуру России исключает возможность признания в его действиях преступления, предусмотренного 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.

Следующей группой проблем является квалификация неоконченной преступной деятельности при совершении преступления, предусмотренного ст. 274^1 УК РФ. Как известно, общее правило о квалификации неоконченного преступления заключается в том, что она должна отражать ту стадию преступления, на которой оно было прервано.

Если учесть, что момент окончания преступления по ч. 2 ст. 274^1 УК РФ согласно тому, как описана его объективная сторона в законе, связывается с наступлением преступных последствий (причинением вреда КИИ России), то остается неясно, как тогда следует оценивать действия лица, осуществившего незаконное проникновение в защищенную систему, однако отказавшегося от непосредственного вмешательства в ее функционирование. Представляется, что в подобной ситуации можно усмотреть признаки добровольного отказа от преступления. Уголовную ответственность в таком случае он может понести только по ч. 1 ст. 274^1 УК РФ, а именно за использование компьютерных программ или компьютерной информации для неправомерного воздействия на КИИ.

Вместе с тем, если лицо совершило неправомерный доступ и блокирование, например, критической информационной инфраструктуры медицинского учреждения, а затем, осознав угрозу для жизни и здоровья пациентов, самостоятельно разблокировало ее, содеянное следует квалифицировать как оконченное преступление по ч. 2 ст. 274[1] УК РФ. Последующие действия виновного, на наш взгляд, образуют признаки деятельного раскаяния виновного, что должно быть учтено в порядке применения ст. 61 УК РФ.

При квалификации действий лица, когда оно намеревалось совершить компьютерную атаку на КИИ, однако по ошибке причинило вред не категорированным объектам, на наш взгляд, необходимо руководствоваться правилом, согласно которому 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.

А. Ю. Решетников и Е. А. Русскевич предлагают руководствоваться следующим квалификационным подходом: «распространение вредоносного программного обеспечения при проведении проверочной закупки с учетом последних разъяснений Пленума Верховного Суда РФ по делам, связанным с незаконным оборотом наркотических средств, следует также оценивать как оконченное преступление»[1].

Данный подход нам представляется уязвимым по ряду причин. Прежде всего, само изменение Пленумом Верховного Суда РФ своей позиции по делам о преступлениях, связанных с незаконным оборотом наркотиков, еще требует своего осмысления и оценки. Известно, что такое решение во многом было обусловлено запросом практики, имело в некотором смысле конъюнктурный характер. С точки зрения науки уголовного права веских доводов в пользу такой квалификации мало. В связи с этим полагаем, что если неправомерное воздействие на КИИ осуществлялось под непосредственным контролем правоохранительных органов (например, в рамках проверочной закупки,

[1] *Решетников А. Ю., Русскевич Е. А*. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации // Уголовное право. 2018. № 2. С. 92.

оперативного эксперимента и т. д.), содеянное необходимо квалифицировать как неоконченное преступление.

До настоящего времени одной из главных проблем квалификации неправомерного воздействия на объекты КИИ России (если не всех преступлений в сфере компьютерной информации) является его оценка по совокупности с другими преступлениями. Данное преступное деяние зачастую выступает лишь способом совершения посягательства на другие охраняемые уголовным законом объекты (жизнь и здоровье человека, общественную безопасность, безопасность конституционного строя Российской Федерации и т. д.). Как справедливо подчеркивается в отечественной теории уголовного права, «преступления в сфере компьютерной информации по своей природе проявляют себя как "инструментальные", поскольку обладают свойством выступать способом достижения иных преступных целей»[1].

Так, в приговоре Ленинского районного суда г. Владивостока от 25 сентября 2019 г. по делу № 1-368/2019 указано, что лицо своими действиями совершило не только неправомерный доступ к компьютерной информации, составляющей коммерческую тайну, но и в последующем распространило указанные сведения (Г. с использованием специальной почтовой программы, установленной на рабочей станции, подключилась к своей личной электронной почте и, создав новое электронное письмо, прикрепила в качестве приложения к нему архив, содержащий сведения, составляющие коммерческую тайну. Это письмо с архивом Г. отправила на электронный почтовый ящик генерального директора сторонней коммерческой организации). Действия виновной получили уголовно-правовую оценку только по ч. 4 ст. 274[1] УК РФ без применения ст. 183 УК РФ.

Системную проблему неполной квалификации при наличии признаков незаконного получения и разглашения сведений, составляющих коммерческую,

---

[1] *Мелешко Д. А., Чернявский Д. О., Шарафетдинова Г. А*. «Инструментальный» характер компьютерных преступлений и его влияние на квалификацию // Законность. 2020. № 3. С. 57.

налоговую или банковскую тайну, справедливо выделяет и обстоятельно анализирует в своей работе Р. Р. Гайфутдинов[1].

В теории уголовного права неоднозначно решается вопрос о квалификации неправомерного воздействия на информационные системы критического значения, если такое деяние было совершено в целях устрашения населения либо подрыва экономической безопасности Российской Федерации. Так, Е. А. Русскевич, по-видимому, исходя из «инструментальной» природы преступлений в сфере компьютерной информации, предлагает квалифицировать содеянное также по совокупности[2]. Указанная точка зрения представляется дискуссионной. Полагаем, что в подобных ситуациях квалификация по ст. 205 и (или) ст. 281 УК РФ с достаточной полнотой охватывает признаки содеянного. Как известно, диспозиции указанных уголовно-правовых норм носят открытый характер в части описания общественно опасного деяния.

Таким образом, исходя из системного толкования, следует сделать вывод, что совершение кибератаки на объекты критической информационной инфраструктуры (транспортные узлы, энергетические системы и т. п.) в террористических и диверсионных целях вполне может быть оценено исключительно в рамках уголовно-правовых норм об ответственности за террористический акт и диверсию.

Изучение правоприменительной практики по делам о неправомерном воздействии на объекты КИИ России позволило выявить и другие квалификационные ошибки. Судебно-следственные органы неверно оценивают действия лица, которое не только использовало вредоносную компьютерную программу, заведомо предназначенную для неправомерного воздействия на объекты критической информационной инфраструктуры Российской Федерации, но и тем самым осуществило неправомерный доступ и модификацию хранящейся в таких объектах компьютерной информации.

---

[1] См.: *Гайфутдинов Р. Р.* Квалификация преступлений против безопасности компьютерной информации : монограф. ... С. 155.

[2] См.: *Русскевич Е. А.* Уголовное право и «цифровая преступность»: проблемы и решения: монограф. … С. 143.

Так, Г. был осужден по ч. 1 ст. 274[1] УК РФ. Согласно приговору суда Г., осознавая (в силу занимаемой должности) необходимость прохождения процедуры тестирования знаний технически-распорядительных актов железнодорожных станций, без которой невозможно получение (продление) допуска к выезду на участок обслуживания, решил пройти указанную процедуру в учебном классе. При этом, стремясь получить гарантированный положительный результат тестирования, Г. решил воспользоваться сторонним нештатным программным обеспечением, предоставляющим тестируемому в модуле «АС ГРАТ» программного комплекса «АСУТ» ОАО «РЖД» получение такого результата независимо от правильности ответов на вопросы теста. В этих целях Г. отыскал в сети «Интернет» вредоносную компьютерную программу «Бот ТРА станций (АС ГРАТ)», заведомо предназначенную для неправомерного воздействия на модуль «АС ГРАТ» программного комплекса «АСУТ» ОАО «РЖД». Г. скопировал эту программу на собственный внешний накопитель (флэш-карту), оплатив 520 руб. через сервис электронных расчетов. В рабочее время Г., имея при себе эту флэш-карту, прибыл в учебный класс, где на служебном персональном компьютере, имеющем подключение к сети передачи данных ОАО «РЖД», приступил к прохождению тестирования знаний технически-распорядительных актов железнодорожных станций. Реализуя свой преступный умысел, направленный на использование компьютерной программы, заведомо предназначенной для неправомерного воздействия на объект критической информационной инфраструктуры Российской Федерации, осознавая общественную опасность и противоправность своих действий, предвидя возможность наступления общественно опасных последствий в виде модификации содержащейся в ней компьютерной информации, Г. при прохождении тестирования подключил собственный внешний накопитель (флэш-карту) к служебному персональному компьютеру и запустил стороннее программное обеспечение — компьютерную программу «Бот ТРА станций (АС ГРАТ)», тем самым совершил умышленные действия, направленные на использование компьютерной программы, заведомо предназначенной для

неправомерного воздействия на модуль «АС ГРАТ». Из-за применения Г. на служебном компьютере нештатного программного обеспечения в виде исполняемых файлов была неправомерно модифицирована компьютерная информация субъекта критической информационной инфраструктуры — ОАО «РЖД» в программном комплексе «АСУТ», сформировав положительный результат его тестирования в модуле «АС ГРАТ»[1].

Полагаем, что в данной ситуации деяние, предусмотренное ч. 1 ст. 274[1] УК РФ, «переросло» в неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, повлекший ее модификацию (ч. 2 ст. 274[1] УК РФ). Диспозиция ч. 2 ст. 274[1] УК РФ содержит признаки составного преступления. В ней указано, что под неправомерным доступом следует также понимать доступ 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. Таким образом, ч. 2 ст. 274[1] УК РФ охватывает и не требует квалифицировать по совокупности неправомерный доступ к объектам критической информационной инфраструктуры, совершенный с использованием заведомо предназначенных для этого вредоносных программ (ч. 1 ст. 274[1] УК РФ) или иных вредоносных программ (ст. 273 УК РФ).

Аналогичная ошибка допущена и в постановлении Невинномысского городского суда Ставропольского края от 16 октября 2020 г. по делу № 1-410/2020[2], из которого следует, что Б., обладая специальными навыками в области работы с ЭВМ и компьютерными программами, в нарушение ст. 16 Федерального закона от 27 июля 2016 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», с целью неправомерного копирования компьютерной информации приобрел: компьютерную программу «MailsBuilder»,

---

[1] Приговор Советского районного суда г. Волгограда от 15 сент. 2020 г. по делу № 1-315/2020 [Электронный ресурс] // Судебные и нормативные акты РФ. URL: www.sudact.ru (дата обращения: 07.08.2022).

[2] URL: www.судебныерешения.рф (дата обращения: 07.08.2022).

относящуюся к вредоносному программному обеспечению, предназначенную для неправомерного воздействия на информационные системы, в том числе и на критическую информационную инфраструктуру Российской Федерации; компьютерную программу «Aparser», предназначенную для автоматизированного получения информации с интернет-ресурсов по заданным критериям и ее дальнейшей обработке; компьютерную программу «Sib Panel», предназначенную для неправомерного воздействия на информационные системы, в том числе и на критическую информационную инфраструктуру Российской Федерации. С целью использования перечисленных вредоносных компьютерных программ, предназначенных для нейтрализации средств защиты компьютерной информации путем перебора логина и пароля, а также для осуществления скрытого неправомерного доступа к компьютерной информации, в том числе и к критической информационной инфраструктуре Российской Федерации, открыл арендованный им сервер. Действуя умышленно и желая проверить функциональные возможности вредоносных компьютерных программ, находясь по месту жительства, осуществил компьютерные атаки типа SQL-инъекций на информационный ресурс, относящийся к информационным системам, автоматизированным системам управления и информационно-телекоммуникационным сетям и являющийся, в соответствии с п. 7 ст. 2 Федерального закона от 26 июля 2019 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», объектом критической информационной инфраструктуры, принадлежащий лаборатории Цитометрии и Биокинетики Института химической кинетики и горения им. В. В. Водоевского Сибирского отделения РАН (г. Новосибирск), который, в соответствии с п. 8 ст. 2 указанного закона, п.п. 1, 2, 3 Устава института (утв. приказом Минобрнауки России от 25 июля 2018 г. № 383), является научной организацией, созданной в форме федерального государственного бюджетного учреждения (субъект критической информационной инфраструктуры), тем самым осуществил неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, повлекшее копирование содержащейся

в ней информации — 505 адресов электронной почты зарегистрированных пользователей с хэш-суммами паролей.

Данный подход к квалификации сохраняется до настоящего времени. Подтверждением тому может служить приговор Харабалинского районного суда Астраханской области от 21 декабря 2022 г. № 1-237/2022, согласно которому при совершении распределенных атак на категорированные сетевые ресурсы с последующим отказом системы и блокированием доступа к информации содеянное было квалифицировано исключительно как использование вредоносной компьютерной информации по ч. 1 ст. 274[1] УК РФ[1]. Соответственно, суд необоснованно оставил без внимания то обстоятельство, что компьютерная атака завершилась причинением вреда КИИ, а само использование вредоносной программы явилось способом осуществления неправомерного доступа, то есть деяния, предусмотренного ч. 2 ст. 274[1] УК РФ. Полагаем, что подобные действия правильно квалифицировать именно как неправомерный доступ к компьютерной информации, хранящейся в категорированном объекте.

Применительно к указанному делу важно также отметить, что лицо после осуществления компьютерной атаки связывалось с представителем компании потерпевшего и выдвигало требования материального характера за прекращение совершаемых им действий. Надо признать, что положения российского законодательства об уголовной ответственности за вымогательство в этом случае не могут быть применимы, поскольку содержанием угрозы является блокирование либо уничтожение компьютерной информации. В отечественной науке уголовного права на эту проблему уже было обращено внимание. Тем не менее до настоящего времени законодателем никакие действия в этом направлении не предпринимались. Как представляется, решением проблемы могло бы стать дополнение диспозиции ст. 163 УК РФ соответствующей оговоркой об угрозе неправомерного уничтожения, модификации либо блокирования компьютерной информации.

---

[1] Архив решений арбитражных судов и судов общей юрисдикции www.sudrf.cnd.ru (дата обращения: 04.04.2023).

И в завершение исследования проблемных вопросов квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации представляется необходимым сформулировать некоторые итоги.

1. Установлено, что неправомерный доступ к КИИ России, 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 КИИ России.

2. Обосновано, что вопрос о пределах вменения при соучастии в неправомерном воздействии на КИИ России должен решаться с учетом объема вины. Заблуждение одного из соучастников относительно направленности совершаемого деяния именно на КИИ России делает невозможной квалификацию 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.

3. Аргументирован вывод о том, что, если лицо намеревалось совершить компьютерную атаку на КИИ России, однако 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.

4. Если неправомерное воздействие на КИИ России осуществлялось под непосредственным контролем правоохранительных органов (в рамках проверочной закупки, оперативного эксперимента и т. д.), содеянное необходимо квалифицировать как неоконченное преступление.

§ 2. Основные направления совершенствования уголовного законодательства об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации

Изучения юридической литературы позволило установить, что в отечественной доктрине уголовного права содержится достаточно много работ, содержащих обстоятельные нарекания относительно конструкции уголовно-правовой нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. В связи с этим авторами формулируются и обосновываются различные решения по тому, как можно было бы скорректировать содержание ст. 274[1] УК РФ. В рамках настоящего исследования оставить обозначенные вопросы без анализа было бы существенным упущением. В связи с этим представляется необходимым рассмотреть те основные направления модернизации исследуемой нормы, которые обосновываются специалистами.

Одним из наиболее принципиальных замечаний, касающихся конструкции ст. 274[1] УК РФ, является то, «что она не учитывает градацию объектов критической информационной инфраструктуры в зависимости от категории значимости в качестве основания дифференциации уголовной ответственности»[1]. Действительно, «подобное решение представляется достаточно логичным, поскольку значимость объекта критической информационной инфраструктуры напрямую влияет на степень общественной опасности совершенного в отношении него неправомерного воздействия. В этом отношении исследуемая норма,

---

[1] См., например: *Решетников А. Ю., Русскевич Е. А*. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274[1] УК России) // Законы России: опыт: анализ, практика. 2018. № 2 (66). С. 55; *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. 135 ; *Кругликов Л. Л., Соловьев О. Г. Бражник С. Д*. Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в системе экономической и информационной безопасности государства // Вестник ЯрГУ. Сер.: Гуманитарные науки. 2019. Т. 4. (50). С. 51.

безусловно, требует доработки. При этом понятно, что все основные составы преступлений, предусмотренные ст. 274[1] УК РФ, будут предполагать совершение посягательства в отношении объектов критической информационной инфраструктуры третьей категории»[1]. Дифференциацию ответственности в этом случае нужно будет проводить в зависимости от совершения посягательства на защищенные информационные объекты второй и первой категорий значимости[2].

Еще одним распространенным замечанием относительно системы квалифицирующих признаков, как уже отмечалось ранее, является отсутствие в ч. 5 ст. 274[1] УК РФ указания на угрозу наступления тяжких последствий. Данный вопрос уже был нами затронут ранее при исследовании объективных признаков неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации. В дополнение следует лишь указать, что корректировка анализируемой нормы в данном отношении позволит выдержать системный (блоковый) подход к дифференциации ответственности за совершение преступлений одной группы.

Минэкономразвития России подготовлен законопроект о внесении изменений в ст. 274[1] УК РФ[3]. «Главной целью данного документа является устранение формально-юридической неопределенности исследуемой нормы. Так, законопроект предполагает отказ от признака причинения вреда критической информационной инфраструктуре по причине его многозначности, что, по мнению разработчиков, «детерминирует высокую степень субъективности при его толковании и последующем применении». Одновременно с этим предлагается включить признак “причинение крупного ущерба”»[4].

---

[1] *Малыгин И. И.* О совершенствовании уголовного законодательства об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Российской правовой академии. 2021. №3. С. 118 – 121.

[2] Данный вывод нашел свою поддержку у 84 % опрошенных респондентов (см. приложение Б, с. 189–193).

[3] Проект федерального закона «О внесении изменений в статью 274[1] Уголовного кодекса Российской Федерации» [Электронный ресурс]. Документ официально опубликован не был. Доступ из справ.-правовой системы «Консультант-Плюс» (дата обращения: 21.01.2023).

[4] *Малыгин И. И.* О совершенствовании уголовного законодательства…

«Понимая, что цель конкретизации признаков состава таким образом будет в определенном смысле достигнута, все же выскажем свое принципиальное несогласие с таким решением. По мнению авторов законопроекта, ответственность за неправомерное воздействие на критическую информационную инфраструктуру должна быть всецело связана с наступлением последствий в виде имущественного ущерба. Столь секвестрированное толкование и возможную (при одобрении документа) формализацию основания уголовной ответственности за посягательство на информационные объекты особой важности сложно комментировать. Посягательство на критическую информационную инфраструктуру, конечно же, может предполагать сугубо экономические потери. Вместе с тем такое деяние может быть связано и с наступлением последствий не имущественных, например, связанных с причинением вреда здоровью человека, последствий экологических, организационных, политических и т. д. При подобных обстоятельствах исследуемая норма работать не будет. Правильно ли это? Полагаем, что ответ на данный вопрос может быть только отрицательный. Нельзя неправомерное воздействие на критическую информационную инфраструктуру государства механически уподоблять преступлениям в сфере экономики»[1].

Проведенный анализ зарубежного законодательства позволил выявить практику криминализации нарушения требований в области обеспечения безопасности КИИ специальным субъектом – лицом, в силу выполняемой им работы или занимаемой должности обязанным соблюдать эти правила.

Данный подход не реализован в отечественном правовом поле. При этом, как нетрудно заключить, положения ст. 274[1] УК РФ, как правило, не распространяются на случаи умышленного неисполнения соответствующих обязанностей либо распространяются в крайне незначительной форме. Закон о безопасности КИИ России также предусматривает обязанности субъектов КИИ: «незамедлительно информировать о компьютерных инцидентах, оказывать

[1] Там же.

содействие должностным лицам федерального регулятора, выполнять их предписания, реагировать на компьютерные инциденты и др.» (ст. 9).

«Неисполнение указанных выше обязанностей соответствующими субъектами объективно причиняет или создает угрозу причинения вреда состоянию защищенности критической информационной инфраструктуры Российской Федерации. В связи с тем что нарушение порядка реагирования на компьютерные инциденты, невыполнение вынесенных предписаний объективно может повлечь наступление тяжких последствий в сфере функционирования информационных объектов особой важности, полагаем, что в данном отношении отечественное уголовное законодательство требует совершенствования. Перспективным видится дополнение гл. 28 УК РФ новой нормой — ст. 274^3 «Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации»[1].

В отечественной теории уголовного права данную идею Е. А. Русскевич обосновывает следующим образом: «… установление уголовной ответственности за уклонение от исполнения отдельных обязанностей лицами, ответственными за обеспечение безопасности объектов критической информационной инфраструктуры, может быть реализовано двумя способами: 1) путем построения соответствующего состава с административной конструкцией; 2) посредством определения состава преступления с материальной конструкцией, включив в качестве криминообразующих признаков причинение крупного ущерба либо наступление тяжких последствий»[2].

«В данном аспекте позиция автора представляется дискуссионной. Реализация первой модели потребует внесения соответствующих изменений в отечественный закон об административных правонарушениях. Кроме того, с учетом специфики исследуемого деяния есть основания полагать, что состав

---

[1] *Малыгин И. И.* О совершенствовании уголовного законодательства…

[2] *Русскевич Е. А.* О совершенствовании уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации // Уголовное право: стратегия развития в XXI веке : материалы XVIII Междунар. науч.-практ. конференции «Уголовное право: стратегия развития в XXI веке» (Москва, МГЮА им. О.Е. Кутафина, 21–22 января 2021 г.). М. : РГ-Пресс, 2021. С. 187–190.

с административной преюдицией просто не будет работать — владелец (оператор) объекта КИИ России будет оперативно менять ответственных исполнителей, делая тем самым невозможным повторность нарушения.

Второе предлагаемое решение представляется сомнительным в том отношении, что соответствующие последствия (причинение крупного ущерба либо наступление тяжких последствий) справедливо использовать как средство дифференциации ответственности. В противном случае возникает обоснованный вопрос — почему уголовная ответственность за нарушение эксплуатационных правил критической информационной инфраструктуры Российской Федерации (ч. 3 ст. 274[1] УК РФ) наступает в зависимости от причинения вреда соответствующим объектам, а при нарушении иных правил безопасности только в случае установления тяжких последствий либо крупного ущерба? Понятно, что логика построения закона здесь объективно страдает»[1].

В связи с этим полагаем, что модель построения нормы об ответственности за нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (в том числе в части пенализации) должна основываться на редакции близкой ей ч. 3 ст. 274[1] УК РФ.

С учетом изложенного предлагаются авторские варианты редакций норм, предусмотренной ст. 274[1] УК РФ, а также проектируемой 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

[1] *Малыгин И. И.* О совершенствовании уголовного законодательства…

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»[1].

Предупреждая возможную критику относительно очередных в ряду многих предложений по изменению уголовного законодательства, хотелось бы заверить, что мы разделяем тезис о необходимости выверенного подхода и стабилизации законопроектной деятельности в сфере уголовно-правовой политики. Действительно, от бесконечного переписывания положений УК РФ зачастую мало практической пользы. Само изменение нормативного поля еще не позволяет сразу же, здесь и сейчас решить социальную проблему. У автора нет наивных ожиданий по этому поводу. При этом негативные последствия, хотя бы на уровне известного раздражения практиков от нескончаемой чехарды поправок в уголовный закон, вполне очевидны.

В этой связи предлагаемые решения по совершенствованию законодательства можно рассматривать как попытку стратегического планирования в конкретной сфере. Уже в ближайшем будущем будет накоплен

[1] Решение о дополнении гл. 28 УК РФ новой нормой, а равно редакция проектируемой ст. 274^3, нашли поддержку у 74 % опрошенных респондентов (см. приложение Б, с. 189–193).

определенный социальный опыт в исследуемой сфере. Есть очень серьезные основания полагать, что он будет свидетельствовать о многочисленных злоупотреблениях владельцев объектов критической информационной инфраструктуры. Если этот прогностический вывод найдет свое подтверждение, нам необходимо будет пойти по пути Сингапура и установить самостоятельную ответственность за соответствующие нарушения.

Важно понимать, что обеспечение эффективной защиты объектов КИИ государства требует комплексного подхода. Необходимо не только сформировать и совершенствовать корпус регулятивного законодательства, но и выстроить механизм государственно-частного партнерства с четким разделением ответственности сторон. В области критически важных технологий, где зачастую субъектами выступают частные компании, это ключевое условие общего успеха. При этом превалирование только репрессивного (уголовно-правового) подхода может иметь обратный эффект, и это обязательно должно учитываться субъектами, определяющими политику государства в данной сфере.

Проведенное исследование позволило также выявить проблему кадрового обеспечения сферы защиты объектов КИИ России. Несмотря на то что в этом направлении государством уже предприняты конкретные меры по повышению привлекательности соответствующего профильного образования и статуса работников в области IT-технологий, «кадровый голод» до настоящего времени является существенным фактором риска. Интервью с экспертами из IT-отрасли свидетельствуют о достаточно сложной ситуации на кадровом рынке, росте существующих угроз, что, соответственно, не способствует повышению эффективности противодействия киберпреступности. Полагаем, что подготовка специалистов в области эксплуатации и защиты объектов КИИ России должна быть основана на многоуровневой системе образования, начальным этапом которой является получение соответствующих знаний в школе.

Цифровая трансформация социальных отношений не завершена. Многие ее аспекты окажут самое непосредственное и значительное влияние на уголовно-

правовую сферу, что, как представляется, повлечет дальнейшее расширение положений гл. 28 УК РФ.

Заключение

Завершая настоящее исследование, хотелось бы отметить, что поставленные цели и задачи выполнены и нашли свое выражение в научно обоснованных положениях, выносимых на защиту. В обобщенном же виде результаты исследования можно представить следующим образом.

Установлено, что реализованная законодателем дифференциация уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации соответствует современным вызовам и угрозам, возникающим на фоне процесса цифровизации жизнедеятельности. Выделение специальной нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации позволило ликвидировать имевшийся дисбаланс в уголовном законе, что дает основание оценить это законодательное решение положительно. Законодатель тем самым обеспечил успешное решение сразу нескольких прикладных задач:

1) решен вопрос, связанный с подследственностью по делам о преступлении, предусмотренном ст. 274^1 УК РФ, — предварительное расследование осуществляется следователями органов Федеральной службы безопасности (в отличие от остальных компьютерных преступлений);

2) созданы предпосылки для индивидуального статистического учета;

3) достигнут максимально возможный предупредительный эффект, вытекающий из самого факта изменения уголовного закона;

4) обеспечена возможность дифференциации уголовной ответственности за само неправомерное воздействие на объекты КИИ.

В технико-юридическом плане дифференциацию уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации нельзя признать оптимальной. При конструировании ст. 274^1 УК РФ допущены серьезные

просчеты, которые снижают эффективность уголовно-правовой охраны отношений, обеспечивающих информационную безопасность.

Теоретически обоснована 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 КИИ.

В настоящее время международное право, применимое к отношениям в сфере обеспечения безопасности КИИ, действует только между ограниченным кругом государств, для которых складывается соответствующая практика в силу регионального (локального) сотрудничества.

В работе показано, что Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере информационных технологий, как основной документ о противодействии цифровой преступности в регионе, требует доработки путем дополнения ст. 3 пунктом «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».

Одновременно с этим представляется необходимым дополнить ст. 1 данного Соглашения понятием объекта информационно-коммуникационной инфраструктуры, под которым следует понимать 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 (гл. 34 УК РФ). Перспективным видится 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.

Установлено, что по способу юридического закрепления уголовной ответственности за неправомерное воздействие на КИИ, уголовные законодательства зарубежных государств можно разделить на три группы:

- страны, где обозначенный вопрос специально не выделен и решается на уровне общих положений об ответственности за преступления в сфере компьютерной информации (Беларусь, Буркина Фасо, Канада, Узбекистан);

- вторую группу образуют уголовные законодательства стран, в которых совершение деяния в отношении критической информационной инфраструктуры выступает квалифицирующим признаком преступлений в сфере компьютерной информации (Австрия, Азербайджан, Германия, Италия, Казахстан, Латвия, Франция);

- третью группу формируют уголовные законодательства государств, включающие специальные нормы об ответственности за неправомерное воздействие на КИИ (Ботсвана, Великобритания, Замбия, Кения, Мальта, Нигерия, США, Уганда).

Зарубежный опыт в части криминализации не «эксплуатационных», а регулятивных требований в области КИИ, представляет значительный теоретический интерес и практический потенциал для российской уголовной политики. Как представляется, исследуемая ст. 274^1 УК РФ, равно как и ст. 274^2 УК РФ, не распространяют свое действие на возможные и имеющие место в объективной действительности случаи злоупотреблений лицами, наделенными управленческими функциями в организациях, владеющих объектами КИИ

(уклонение от категорирования, занижение категории значимости, уклонение от сообщения о компьютерных инцидентах и т. п.).

Доказано, 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.

Аргументировано положение о том, что предметом преступления, предусмотренного ст. 274[1] УК РФ, является значимый объект критической информационной инфраструктуры (независимо от категории значимости), характеризующийся двумя критериями:

а) *критерием значимости*, то есть социальной, политической, экономической, экологической или оборонной важности;

б) *реестровым критерием*, связанным с включением объекта в реестр значимых объектов КИИ.

При этом важно, что для признания соответствующего объекта информационной инфраструктуры предметом преступления, предусмотренного ст. 274[1] УК РФ, необходимо наличие обоих указанных критериев.

Обоснован вывод о том, что по смыслу ч. 2 ст. 274[1] УК РФ под вредом следует понимать:

1) нарушение функционирования объекта критической информационной инфраструктуры;

2) прекращение функционирования объекта критической информационной инфраструктуры;

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

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

5) нарушение безопасности обрабатываемой таким объектом информации.

В работе приведено обоснование тезиса о том, что толкование служебного положения лица как квалифицирующего признака неправомерного воздействия на КИИ носит двойственный характер:

а) применительно к ч. 1 и ч. 2 ст. 274[1] УК РФ оно должно быть расширительным — в качестве такого лица может выступать любое лицо, которое обязано в силу выполняемых им профессиональных функций соблюдать и (или) обеспечивать информационную безопасность объектов КИИ России;

б) в отношении деяния, описанного в 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 действия лица были направлены на вмешательство в функционирование программных или программно-аппаратных средств, которые субъектом не были категорированы и, соответственно, не были включены ФСТЭК в Реестр, содеянное не может оцениваться в рамках ст. 274[1] УК РФ и требует квалификации по ст. 272 УК РФ. Данным правилом необходимо руководствоваться и при разрешении вопросов об обратной силе уголовного закона.

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 статье при условии, что допущенные ими нарушения специальных правил находились в причинной связи с наступившими последствиями.

Аргументировано положение о том, что 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.

Следует считать доказанным, что если лицо 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 следует как повлекшее наступление тяжких последствий, то есть по ч. 4 ст. 272 УК РФ.

Вопрос о пределах вменения при соучастии в неправомерном воздействии на КИИ России 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 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.

Установлено, что неправомерный доступ к КИИ России, 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 КИИ России;

Аргументирован вывод о том, что если лицо намеревалось совершить компьютерную атаку на КИИ России, 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;

С учетом полученных результатов исследования предлагается внести изменения в ст. 274^1 УК РФ, а также установить ответственность за нарушение требований в области безопасности КИИ России, дополнив Уголовный кодекс РФ новой нормой — ст. 274^3, авторская редакция которой представлена в работе (приложение Б, с. 189–193).

Обеспечение эффективной защиты объектов КИИ государства является важным элементом построения и развития электронного правительства и цифровой экономики. Подтверждением этому выступает недавняя криминализация действий, связанных с эксплуатацией технических средств противодействия угрозам киберустойчивости (ст. 274^2 УК РФ) — мера, очевидной целью которой является защита российского сегмента сети «Интернет». Решение данной задачи требует комплексного подхода. Необходимо не только сформировать и совершенствовать корпус регулятивного законодательства, но и выстроить механизм государственно-частного партнерства с четким разделением ответственности сторон. В области критически важных технологий, где зачастую субъектами выступают частные компании, это ключевое условие общего успеха. При этом превалирование только репрессивного (уголовно-правового) подхода может иметь обратный эффект и обязательно должно учитываться субъектами, определяющими политику государства в данной сфере.

Проведенное исследование позволило также выявить проблему в кадровом обеспечении в сфере защиты объектов КИИ России. Несмотря на то, что в этом направлении государством уже предприняты конкретные меры по повышению привлекательности соответствующего профильного образования и статуса работников в области IT-технологий, «кадровый голод» до настоящего времени является существенным фактором риска. Как и во многих других отраслях, система подготовки специалистов в области эксплуатации и защиты объектов КИИ должна быть построена на основе многоуровневой системы обучения

и образования, начальным этапом которой является получение соответствующих знаний в школе.

Библиографический список

Нормативные правовые акты, официальные документы Российской Федерации

1. **Российская Федерация. Законы.** Конституция Российской Федерации : принята всенародным голосованием 12 декабря 1993 года (с учетом поправок, внесенных законами Российской Федерации о поправках к Конституции Российской Федерации от 30 декабря 2008 года № 6-ФКЗ, от 30 декабря 2008 года № 7-ФКЗ, 5 февраля 2014 года № 2-ФКЗ, от 21 марта 2014 года № 1-ФКЗ, от 21 июля 2014 года № 11-ФКЗ, от 14 марта 2020 года № 1-ФКЗ, от 4 октября 2022 года № 5-ФКЗ, 6-ФКЗ, 7-ФКЗ, 8-ФКЗ. — Текст : электронный // Российская газета — 1993, 25 дек. ; Официальный интернет-портал правовой информации www.pravo.gov.ru, 06.10.2022 (дата обращения: 15.01.2023).

2. **Российская Федерация. Законы.** Уголовный кодекс Российской Федерации : УК : текст изменениями и дополнениями на 18 марта 2023 года : [Федеральный закон от 13 июня 1996 года № 63-ФЗ : принят Государственной думой 24 мая 1996 года : одобрен Советом Федерации 5 мая 1996 года]. — Текст : электронный // Собрание законодательства Российской Федерации. — 1996. — № 25, ст. 2954 ; Официальный интернет-портал правовой информации www.pravo.gov.ru, 18.03.2023 (дата обращения: 14.04.2023).

3. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 года № 149-ФЗ : [принят Государственной думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года : в редакции от 22 декабря 2022 года]. — Текст : электронный // Собрание законодательства Российской Федерации — 2006. — № 31 (часть I), ст. 3448 ; Официальный интернет-портал правовой информации www.pravo.gov.ru, 29.12.2022 (дата обращения: 04.04.2023).

4. **Российская Федерация. Законы.** О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон от 26 июля 2017 года № 187-ФЗ : [принят Государственной думой 12 июля 2017 года : одобрен Советом Федерации 19 июля 2017 года : вступил в законную силу с 1 января 2018 года]. — Текст : электронный // Официальный интернет-портал правовой информации www.pravo.gov.ru, 26.07.2017 (дата обращения: 25.10.2022).

5. **Российская Федерация. Законы.** 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 года № 194-ФЗ : [принят Государственной думой 12 июля 2017 года : одобрен Советом Федерации 19 июля 2017 года : вступил в законную силу с 1 января 2018 года]. — Текст : электронный // Официальный интернет-портал правовой информации www.pravo.gov.ru, 26.07.2017 (дата обращения: 16.10.2021).

6. **Российская Федерация. Законы.** О внесении изменений в Уголовный кодекс Российской Федерации : Федеральный закон от 18 марта 2023 года № 82-ФЗ : [принят Государственной думой 14 марта 2023 года : одобрен Советом Федерации 15 марта 2023 года]. — Текст : электронный // Официальный интернет-портал правовой информации www.pravo.gov.ru, 18.03.2023 (дата обращения: 14.04.2023).

7. Об утверждении Перечня сведений конфиденциального характера : Указ Президента Российской Федерации от 6 марта 1997 г. № 188 : в редакции Указа от 13 июля 2015 года № 357. — Текст : электронный // Собрание законодательства Российской Федерации. — 1997. — № 10, ст. 1127 ; Официальный интернет-портал правовой информации www.pravo.gov.ru, 13.07.2015 (дата обращения: 20.12.2021).

8. Об утверждении Доктрины информационной безопасности Российской Федерации : Указ Президента Российской Федерации от 5 декабря 2016 года

№ 646. — Текст : электронный // Официальный интернет-портал правовой информации www.pravo.gov.ru, 06.12.2016 (дата обращения: 11.11.2021).

9. О Об утверждении Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : Указ Президента Российской Федерации от 9 мая 2017 года № 203. — Текст : электронный // Официальный интернет-портал правовой информации www.publication.pravo.gov.ru, 10.05.2017 (дата обращения: 04.12.2021).

10. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных : постановление Правительства Российской Федерации от 1 ноября 2012 года № 1119. — Текст : электронный // Собрание законодательства Российской Федерации. — 2012. — № 45, ст. 6257. — URL: www.consultant.ru (дата обращения: 15.03.2022).

11. Об утверждении правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : постановление Правительства Российской Федерации от 8 февраля 2018 года № 127 : в редакции постановления от 20 декабря 2022 года № 2360. — Текст : электронный // Официальный интернет-портал правовой информации www.publication.pravo.gov.ru, 13.02.2018, 21.12.2022 (дата обращения: 25.01.2023).

12. Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : приказ ФСТЭК России от 11 февраля 2013 года № 17 (зарег. в Минюсте России 31 мая 2013 года, рег. № 28608) : в редакции, действующей с 1 января 2021 года. — Текст : электронный // Электронный фонд правовых и нормативно-технических документов. — URL: www.docs.cntd.ru (дата обращения: 22.12.2022).

13. Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации : приказ ФСТЭК России от 6 декабря 2017 года № 227 : (зарег. в Минюсте России

8 февраля 2017 года, рег. № 49966). — Текст : электронный // Официальный интернет-портал правовой информации www.publication.pravo.gov.ru, 09.02.2017 (дата обращения: 12.10.2022).

14. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации : Приказ ФСТЭК России от 25 декабря 2017 года № 239 (зарег. в Минюсте России 26 марта 2018 года, рег. № 50524). — Текст : электронный // Официальный интернет-портал правовой информации www.publication.pravo.gov.ru, 27.03.2018 (дата обращения: 17.06.2022).

15. О внесении изменений в Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 25 декабря 2017 г. № 239 : приказ ФСТЭК России от 20 февраля 2020 года № 35 (зарег. в Минюсте России 11 сентября 2020 года № 59793). — Текст : электронный // Официальный интернет-портал правовой информации www.publication.pravo.gov.ru, 14.09.2020 (дата обращения: 17.06.2022).

16. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации. — Текст : электронный // Документы – Генеральная прокуратура Российской Федерации : сайт. — URL: www.epp.genproc.gov.ru, 14.04.2014 (дата обращения: 10.09.2022).

17. Пояснительная записка Правительства Российской Федерации к проекту федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации. — Текст : электронный // Система обеспечения законодательной деятельности : сайт. — URL: www.sozd.duma.gov.ru. (дата обращения: 15.11.2022).

18. Пояснительная записка Правительства Рос. Федерации к проекту федерального закона № 47591-7 «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской

Федерации в связи с принятием Федерального закона "О безопасности критической информационной инфраструктуры Российской Федерации"». — Текст : электронный // Система обеспечения законодательной деятельности : сайт. — URL: www.sozd.duma.gov.ru. (дата обращения: 20.10.2021).

19. Проект федерального закона «О внесении изменений в статью 274[1] Уголовного кодекса Российской Федерации» : подготовлен Минэкономразвития России, ID проекта 04/13/05-20/00102094). — Текст : электронный. Документ официально опубликован не был. Доступ из справочно-правовой системы «Консультант-Плюс». (дата обращения: 21.01.2023).

Международные нормативные правовые акты

20. Декларация принципов «Построение информационного общества – глобальная задача в новом тысячелетии» от 12 декабря 2003 года. — Текст : электронный // Официальный сайт ООН. — URL: www.un.org (дата обращения: 02.02.2022).

21. Резолюция 56-й сессии ООН A/RES/56/121 от 23 января 2002 года «Борьба с преступным использованием информационных технологий». — Текст электронный // Официальный сайт ООН. — URL: www.un.org (дата обращения: 04.02.2022).

22. Резолюция 57-й сессии ООН A/RES/57/53 от 30 декабря 2002 года «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». — Текст электронный // Официальный сайт ООН. — URL: www.un.org (дата обращения: 05.02.2022).

23. Резолюция 64-й сессии ООН A/RES/64/211 от 21 декабря 2009 года «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур». — Текст электронный // Официальный сайт ООН. — URL: www.un.org (дата обращения: 10.01.2023).

24. Конвенция о преступности в сфере компьютерной информации ETS № 185 от 23 ноября 2001 года. Документ официально опубликован не был. Доступ из справочно-правовой системы «КонсультантПлюс». — Текст : электронный. — URL: www.consultantplus.helpline.ru (дата обращения: 10.02.2022).

25. Конвенция о борьбе с преступлениями в области информационных технологий Лиги арабских государств от 21 декабря 2010 года. — Текст : электронный // League of Arab States, 2010. Arab Convention on Combating Information Technology Offences. — URL: http://www.arableagueonline.org (дата обращения: 20.02.2023).

26. Директива Европейского парламента и Совета ЕС от 12 августа 2013 года № 2013/40/ЕС «Об атаках на информационные системы и о замене Рамочного решения 2005/222/ПВД Совета ЕС» — Текст : электронный // Official Journal of the European Union. — 2013. № L 218. — URL: http://eur-lex.europa.eu (дата обращения: 03.03.2023).

27. Рамочное решение Совета ЕС от 24 октября 2008 года 2008/841/ПВД «О борьбе с организованной преступностью». Текст документа официально опубликован не был. Доступ из справочно-правовой системы «КонсультантПлюс». — Текст : электронный. — URL: www.consultantplus.helpline.ru (дата обращения: 15.03.2022).

28. Модельный закон «О критически важных объектах информационно-коммуникационной инфраструктуры : постановление Межпарламентской Ассамблеи государств – участников СНГ от 28 ноября 2014 года № 41-14. — Текст : электронный // Информационный бюллетень Межпарламентской Ассамблеи государств – участников СНГ. — 2015. — № 62 (часть 2). — URL: www.base.garant.ru (дата обращения: 17.03.2022).

29. Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 года. — Текст : электронный // МИД России : официальный сайт. — URL: www.mid.ru, 06.06.2001 (дата обращения: 25.02.2022).

30. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества (ШОС) о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года. — Текст : электронный // Бюллетень международных договоров. — 2012. — № 1. — С. 13–21. — URL: www.base.garant.ru (дата обращения: 01.03.2022).

31. Соглашение между Правительством Российской Федерации и Правительством Республики Куба «О сотрудничестве в области обеспечения международной информационной безопасности» от 11 июля 2014 года. — Текст : электронный // Бюллетень международных договоров. — 2015. — № 4. — С. 58–64. — URL: www.base.garant.ru (дата обращения: 26.02.2022).

32. Соглашение между Правительством Российской Федерации и Правительством Китайской Народной Республики «О сотрудничестве в области обеспечения международной информационной безопасности» от 8 мая 2015 года. — Текст : электронный // Бюллетень международных договоров. — 2016. — № 11. — С. 82–88. — URL: www.base.garant.ru (дата обращения: 03.03.2022).

33. Соглашение между Правительством Российской Федерации и Правительством Республики Индии «О сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий» от 15 октября 2016 года. — Текст : электронный // Бюллетень международных договоров. — 2017. — № 4. — URL: www.base.garant.ru (дата обращения: 05.03.2022).

34. Соглашение между Правительством Российской Федерации и Правительством Южно-Африканской Республики «О сотрудничестве в области обеспечения международной информационной безопасности» от 4 сентября 2017 года. — Текст : электронный // Официальный сайт МИД России. — URL: www.mid.ru (дата обращения: 10.09.2022).

35. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018 года. — Текст : электронный // Единый реестр

правовых актов и других документов СНГ. — URL: http://cis.minsk.by (дата обращения: 02.02.2023).

36. О Стратегии обеспечения информационной безопасности государств – участников Содружества Независимых Государств : решение Совета глав правительств СНГ от 25 октября 2019 года. — Текст : электронный // Единый реестр правовых актов и других документов СНГ. — URL: http://cis.minsk.by (дата обращения: 17.03.2022).

37. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникации в контексте международной безопасности. Записка Генерального секретаря ООН от 24 июня 2013 года. A/68/98. — Текст : электронный. — URL: https://www.un.org (дата обращения: 12.02.2022).

Зарубежное законодательство

38. Свод законов США. — Текст : электронный. — URL: https://www.law.cornell.edu/uscode/text/18 (дата обращения: 06.05.2022).

39. Уголовный кодекс Норвегии (1842 г., с изм.). — Текст : электронный. — URL: http://www.un.org/depts/los//NOR.penal_code (дата обращения: 24.09.2021).

40. Уголовный кодекс Федеративной Республики Германия (1871 г., с изм.). — Текст : электронный // Федеральный правовой портал «Юридическая Россия». — URL: www.law.edu.ru (дата обращения: 11.02.2023).

41. Уголовный кодекс Республики Мальта (1854 г., с изм.). — Текст : электронный. — URL: www.legislationline.org/download/id/8555/file/Malta_Criminal_Code_amDec 2019_en.pdf (дата обращения: 21.02.2023).

42. Уголовный кодекс Нидерландов (1886 г., с изм.). — Текст : электронный. — URL: http://legislationline.org/documents/section/criminal-codes (дата обращения: 04.10.2021).

43. Уголовный кодекс Финляндии (1889 г., с изм.) : в редакции 2018 года — Текст : электронный. — URL: http://legislationline.org/documents/

section/criminal-codes (дата обращения: 07.10.2021).

44. Уголовный кодекс Италии (1930 г., с изм.). — Текст : электронный. — URL: www.europam.eu/?module=legislation&country=Italy (дата обращения: 05.02.2023).

45. Уголовный кодекс Австрии (1974 г. с изм.). — Текст : электронный. — URL: www.unodc.org/cld/document/aut/1974/austrian_penal (дата обращения: 21.02.2023).

46. Уголовный кодекс Франции (1992 г. с изм.). — Текст : электронный // Российский правовой портал «Библиотека Пашкова». — URL: www.constitutions.ru (дата обращения: 11.02.2023).

47. Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года № 2012-XII (с изм.) : в редакции от 19 октября 2022 года. — Текст : электронный // Законодательство стран СНГ : электронная база данных. — URL: www.baze.spinform.ru (дата обращения: 04.04.2023).

48. Уголовный кодекс Буркина Фасо (1996 г., с изм.). — Текст : электронный. — URL: www.policinglaw.info/assets/downloads/Code_pénal de_Burkina_Faso_(2018).pdf (дата обращения: 08.03.2023).

49. Уголовный кодекс Китайской Народной Республики : принят на 5-й сессии Всекитайского собрания народных представителей шестого созыва 14 марта 1997 года (с изм.) : в редакции от 26 декабря 2020 года. — Текст : электронный // Посольство КНР в Российской Федерации : сайт. — URL: www.ru.china-embassy.gov.ch (дата обращения: 22.10.2022).

50. Уголовный кодекс Республики Польша (1997 г., с изм.). — Текст : электронный. — URL: www.legislationline.org/download/id/7354/file/Poland_CC_1997_en.pdf (дата обращения: 24.02.2023).

51. Уголовный кодекс Латвийской Республики (1998 г., с изм.). — Текст : электронный. — URL: http://legislationline.org/download/action/download/id/4796/file/Latvia_CC_am2013_lt.pdf (дата обращения: 01.11.2021).

52. Уголовный кодекс Республики Беларусь от 9 июля 1999 года № 275-З (с изм.) : [принят Палатой представителей 2 июня 1999 года : одобрен Советом

Республики 24 июня 1999 года: в редакции от 9 марта 2023 года]. — Текст : электронный // Законодательство стран СНГ : электронная база данных. — URL: www.baze.spinform.ru (дата обращения: 04.04.2023).

53. Уголовный кодекс Азербайджанской Республики от 30 декабря 1999 года (с изм.) : в редакции от 29 ноября 2022 года. — Текст : электронный // Законодательство стран СНГ : электронная база данных. — URL: www.base.spinform.ru (дата обращения: 24.02.2023).

54. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V ЗРК (с изм.) : в редакции от 5 ноября 2022 года // Законодательство стран СНГ : электронная база данных. — URL: www.base.spinform.ru (дата обращения: 10.03.2023).

55. Уголовный кодекс штата Луизиана. — Текст : электронный. — URL: https://law.justia.com/codes/louisiana/2015/code-revisedstatutes/title-14/rs-14-61 (дата обращения: 04.04.2022).

56. Закон Великобритании о неправомерном использовании компьютеров 1990 г. (Compu ter misuse act 1990). — Текст : электронный. — URL: www.legislation.gov.uk/ukpga/1990/18/section/3ZA (дата обращения: 11.02.2023).

57. Закон Сингапура о неправомерном использовании компьютерных технологий (1993 г.). — Текст : электронный. — URL: https://sso.agc.gov.sg/Act/CMA1993?ValidDate=20180831&ProvIds=pr9 (дата обращения: 04.02.2023).

58. Акт о защите информационной и коммуникационной инфраструктуры Южной Кореи (2001 г.). — Текст : электронный. — URL: www.elaw.klri.re.kr/eng_mobile/viewer.do?hseq=28812&type=part&key=43 (дата обращения: 31.03.2023).

59. Закон Королевства Саудовская Аравия о противодействии киберпреступности 2007 г. (Anti Cyber Crime Law 2007). — Текст : электронный. — URL: https://www.citc.gov.sa/en/RulesandSystems/CITCSystem/Pages/CybercrimesAct.aspx (дата обращения: 17.11.2021).

60. Закон Уганды «О неправомерном использовании компьютерных

технологий» (2011 г.). — Текст : электронный. — URL: www.nita.go.ug/sites/default/files/publications/Computer%20Misuse%20Act%20%202011%20%28Act%20No.%202%20of%202011%29.pdf (дата обращения: 08.02.2023).

61. Закон Республики Филиппины о предупреждении киберпреступности (2012 г.). — Текст : электронный. — URL: www.ru-zahn-info-portal-de (дата обращения: 11.11.2022).

62. Закон Нигерии «О киберпреступности» (2015 г.). — Текст : электронный. — URL: https://www.cert.gov.ng/ngcert/resources/CyberCrime_Prohibition_Prevention_etc_Act_2015.pdf (дата обращения: 11.02.2023).

63. Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» : в редакции от 5 ноября 2022 года // Законодательство стран СНГ : электронная база данных. — Текст : электронный. — URL: www.base.spinform.ru (дата обращения: 24.02.2023).

64. Закон Южно-Африканской Республики «О кибербезопасности и киберпреступности» (2017 г.). — Текст : электронный. — URL: https://www.gov.za/sites/default/files/gcis_document/201703/b6-2017cybercrimes170221a.pdf (дата обращения: 08.02.2023).

65. Закон Ботсваны о киберпреступности и компьютерных преступлениях (2018 г.). — Текст : электронный. — URL: www.bocra.org.bw/sites/default/files/documents/18%20Act%2029-06-2018%20Cybercrime%20and%20Computer%20Related%20Crimes.pdf (дата обращения: 08.03.2023).

66. Закон Кении «О противоправном использовании компьютерных технологий и киберпреступности» (2018 г.) — Текст : электронный. — URL: www.kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%205%20of%202018 (дата обращения: 08.02.2023).

67. Закон Народной Республики Бангладеш о цифровой безопасности (2018 г.). — Текст : электронный. — URL: www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf (дата обращения:

22.03.2023).

68. Закон Сингапура о кибербезопасности (2018 г.). — Текст : электронный. — URL: www.sso.agc.gov.sg/Acts-Supp/92018/Publishend (дата обращения: 04.02.2023).

69. Закон Замбии «О неправомерном использовании компьютера в преступных целях» (2021). — Текст : электронный. — URL: www.zambialii.org/zm/legislation/act/2004/13/cmaca2004379.pdf (дата обращения: 08.02.2023).

70. Директива (ЕО) PDD-21 и Указ Президента США № 13636 «Об улучшении кибербезопасности критически важной инфраструктуры» (2013 г.) // The White House [Official website]. — Текст : электронный. — URL: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improvingcritical-infrastructure-cybersecurity (дата обращения: 11.09.2021).

71. Указ Президента США № 13800 «Об усилении кибербезопасности федеральных сетей и критически важной инфраструктуры» (2017 г). — Текст : электронный. — URL : https://www.govinfo.gov/content/pkg/DCPD-201700327/pdf/DCPD-201700327.pdf (дата обращения: 20.09.2021).

72. Национальная стратегия Канады по критически важной инфраструктуре вместе с поддерживающим Планом действий по критической инфраструктуре (2009 г.). — Текст : электронный. — URL: https://www.canada.ca/en/services/defence/national_security/criticalinfrastructure.html (дата обращения: 06.05.2022).

73. Парижский призыв к доверию и безопасности в киберпространстве от 12 ноября 2018 года. — Текст : электронный. — URL: www.diplomatie.gouf.fr (дата обращения: 06.10.2022).

74. Bericht zur Lage der IT-Sicherheit in Deutschland 2014. — Текст : электронный. — URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf (дата обращения: 15.04.2022).

Материалы судебной практики

75. О судебной практике по делам о преступлениях, связанных с наркотическими средствами, психотропными, сильнодействующими и ядовитыми веществами : постановление Пленума Верховного Суда Российской Федерации от 15 июня 2006 года № 14 : в редакции от 16 мая 2017 года. — Текст : электронный // Верховный Суд Российской Федерации : сайт. — URL: www.vsrf.ru (дата обращения: 10.03.2023).

76. О судебной практике по делам о мошенничестве, присвоении и растрате : постановление Пленума Верховного Суда Российской Федерации от 30 ноября 2017 года № 48 : в редакции от 15 декабря 2022 года. — Текст : электронный // Верховный Суд Российской Федерации : сайт. — URL: www.vsrf.ru (дата обращения: 10.03.2023).

77. 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 Российской Федерации от 15 декабря 2022 года № 37. — Текст : электронный // Верховный Суд Российской Федерации : сайт. — URL: www.vsrf.ru (дата обращения: 04.04.2023).

78. Апелляционное определение Астраханского областного суда от 14 апреля 2022 года № 22-787/2022. — Текст : электронный // Судебные и нормативные акты РФ : сайт. — URL: www.sudact.ru (дата обращения: 05.11.2022).

79. Постановление Невинномысского городского суда Ставропольского края от 16 октября 2020 года по делу № 1-410/2020. — Текст : электронный // Судебные решения РФ : электронная база данных. — URL: www.судебныерешения.рф (дата обращения: 07.08.2022).

80. Приговор Останкинского районного суда г. Москвы от 4 декабря 2017 года по делу №1-507/17. — Текст : электронный // Официальный портал судов общей юрисдикции города Москвы. — URL: www.mos-gorsud.ru (дата обращения: 07.08.2022).

81. Приговор Октябрьского районного суда г. Красноярска от 11 января 2018 года по делу № 1-108/2018. — Текст : электронный // Судебные решения РФ : электронная база данных. — URL: www.судебныерешения.рф (дата обращения: 25.10.2022).

82. Приговор Люблинского районного суда г. Москвы от 16 мая 2018 года по делу № 01-0289/2018. — Текст : электронный // Официальный портал судов общей юрисдикции города Москвы. — URL: www.mos-gorsud.ru (дата обращения: 14.12.2022).

83. Приговор Ленинского районного суда г. Тамбова от 19 июня 2018 года по делу № 1-91/2018. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 20.01.2023).

84. Приговор Октябрьского районного суда г. Тамбова от 15 февраля 2019 года по делу № 1-134/2019. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 22.01.2021).

85. Приговор Ленинского районного суда г. Владивостока от 25 сентября 2019 года по делу № 1-368/2019. — Текст : электронный // Судебные решения РФ : электронная база данных. — URL: www.судебныерешения.рф (дата обращения: 20.01.2021).

86. Приговор Первомайского районного суда г. Владивостока от 25 сентября 2019 года по делу № 1-376/2019. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 20.01.2021).

87. Приговор Благовещенского городского суда Амурской области от 26 июня 2020 года по делу № 1-536/2020. — Текст : электронный // Судебные решения РФ : электронная база данных. — URL: www.судебныерешения.рф (дата

обращения: 20.12.2022).

88. Приговор Абаканского городского суда Республики Хакасия от 29 июля 2020 года по делу № 1-805/2020. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 20.12.2022).

89. Приговор Советского районного суда г. Волгограда от 15 сентября 2020 года по делу № 1-315/2020. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 07.08.2022).

90. Приговор Ленинского районного суда г. Владивостока от 7 октября 2020 года по делу № 1-366/2020. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 03.03.2023).

91. Приговор Брянского районного суда Брянской области от 28 апреля 2022 года по делу № 1-14/2022. — Текст : электронный // Судебные решения РФ : электронная база данных. — URL: www.судебныерешения.рф (дата обращения: 22.10.2022).

92. Приговор Бежицкого районного суда г. Брянска от 5 августа 2022 года по делу № 1-240/2022. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 10.12.2022).

93. Приговор Октябрьского районного суда г. Владимира от 21 ноября 2022 года по делу № 1-351/2022. — Текст : электронный // Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru (дата обращения: 03.03.2023).

94. Приговор Харабалинского районного суда Астраханской области от 21 декабря 2022 года № 1-237/2022. — Текст : электронный // Архив решений арбитражных судов и судов общей юрисдикции. — URL: www.sudrf.cnd.ru (дата обращения: 04.04.2023).

Специальная научная, учебная литература, монографии

95. **Бикмурзин, М. П**. Предмет преступления: теоретико-правовой анализ / М. П. Бикмурзин. — Москва : Юрлитинформ, 2006. — 183 с. — ISBN 5-93295-226-1. — Текст : непосредственный.

96. Блокчейн на пике хайпа: правовые риски и возможности / А. Ю. Иванов (рук. авт. кол.), М. Л. Башкатов, Е. В. Галкова и др. ; НИУ «Высшая школа экономики», Институт права и развития ВШЭ – Сколково. — Москва : Изд. Дом Высшей школы экономики, 2017. — 237 с. — 500 экз. —ISBN 978-5-7598-1768-0. — Текст : непосредственный.

97. **Букалерова, Л. А**. Уголовно-правовая охрана официального информационного оборота / Л. А. Букалерова ; под редакцией В. С. Комиссаров, Н. И. Пикуров. — Москва : Юрлитинформ, 2006. — 354 с. — ISBN 5-93295-215-6. — Текст : непосредственный.

98. **Гайфутдинов, Р. Р.** Квалификация преступлений против безопасности компьютерной информации : монография / Р. Р. Гайфутдинов ; научный редактор доктор юридических наук, профессор М. В. Талан. — Москва : Юрлитинформ, 2019. — 200 с. — Библиогр. : с. 184–196. — 3000 экз. — ISBN 978-5-4396-1738-8. — Текст : непосредственный.

99. **Дремлюга, Р. И**. Интернет-преступность : монография / Р. И. Дремлюга ; Минобрнауки России, Федеральное агентство по образованию, Дальневосточный гос. университет. — Владивосток : Изд-во Дальневосточного ун-та, 2008. — 240 с. — Библиогр. : с. 224–239. — 300 экз. — ISBN 978-5-7444-2114-4. — Текст : непосредственный.

100. **Евдокимов, К. Н**. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты / К. Н. Евдокимов. — Иркутск : Иркутский юридический ин-т (фил.) Акад. Генеральной прокуратуры РФ, 2016. — 267 с. — 100 экз. — ISBN 978-5-93928-059-4. — Текст : непосредственный.

101. **Жалинский, А. Э.** Уголовное право в ожидании перемен: теоретико-

инструментальный анализ. — изд. 2-е, перераб. и доп. / А. Э. Жалинский. — Москва : Проспект, 2016. — 400 с. — ISBN 978-5-392-20771-8. — Текст : непосредственный.

102. **Козаев, Н. Ш.** Современные технологии и проблемы уголовного права (анализ зарубежного и российского законодательства) : монография / Н. Ш. Козаев ; под редакцией А. В. Наумова. — Москва : Юрлитинформ, 2015. — 217 с. — Библиогр. : с. 172 — ISBN 978-5-4396-0942-0. — Текст : непосредственный.

103. **Кудрявцев, В. Н.** Общая теория квалификации преступлений / В. Н. Кудрявцев. — 2-е изд., перераб. и доп. — Москва : Юристъ, 2006. — 301с. — ISBN 5-7975-0170. — Текст непосредственный.

104. **Мирошниченко, Н. В.** Теоретические основы уголовной ответственности за преступления, связанные с нарушением специальных функций : монография / Н. В. Мирошниченко. — Москва : Юрлитинформ, 2014. — 380 с. — ISBN 978-5-4396-0670-2. — Текст : непосредственный.

105. **Овчинский, В. С.** Криминология цифрового мира : учебник для магистратуры / В. С. Овчинский. — Москва : Норма: ИНФРА-М, 2018. — 352 с. — Библиогр. : с. 11. — ISBN 978-5-91768-896-1 (Норма). — 150 экз. — Текст : непосредственный.

106. **Пикуров, Н. И**. Квалификация преступлений с бланкетными признаками состава : монография / Н. И. Пикуров. — Москва : Российская академия правосудия, 2009. — 288 с. — Библиогр. : с. 138, 210. — ISBN 978-5-93916-184-8. — Текст : непосредственный.

107. **Попов, А. Н.** Преступления в сфере компьютерной информации : учебное пособие / А. Н. Попов. — Санкт-Петербург : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. — 68 с. — УДК 343.3/.7(075). — Библиогр. : с. 64–67. — Текст : непосредственный.

108. **Простосердов, М. А.** Система санкций Особенной части Уголовного кодекса Российской Федерации: анализ, проблемы, пути решений : монография / М. А. Простосердов. — Москва : РГУП, 2020. — 340 с. — Библиогр. : с. 7. — ISBN 978-5-93916-873-1. — Текст : непосредственный.

109. **Пудовочкин, Ю. Е**. Учение о составе преступления : учебное пособие / Ю. Е. Пудовочкин. — Москва : Юрлитинформ, 2009. — 248 с. — Библиогр. : с. 223. — ISBN 978-5-93295-547-5 (в пер.) — Текст : непосредственный.

110. **Рарог, А. И.** Проблемы квалификации преступлений по субъективным признакам : монография [основы общей теории квалификации преступлений, основы учения о субъективной стороне преступления, квалификация преступлений по признакам субъективной стороны, квалификация преступлений по признакам субъекта] / А. И. Рарог. — Москва : Проспект, 2015. — 229 с. — ISBN 978-5-392-18102-5. — Текст : непосредственный.

111. **Русскевич, Е. А.** Уголовное право и «цифровая преступность»: проблемы и решения : монография / Е. А. Русскевич. — Москва : ИНФРА-М, 2019. — 227 с. — Библиогр. : с. 32, 139, 140, 143. — 500 экз. — ISBN 978-5-16-107103-8 (print). — Текст : непосредственный.

112. Сборник исследований по практической безопасности. — Москва : АО «Позитив Текнолоджиз», 2018. — 204 с. — Текст электронный. — URL: www.ptsecurity.kom (дата обращения: 02.03.2023).

113. Уголовное право России. Общая и Особенная части : учебное пособие / под реакцией доктора юридических наук, профессора В. К. Дуюнова. — 6-е изд. — Москва : РИОР: ИНФРА-М, 2019. — 780 с. — Библиогр. : с. 664, 665. — 500 экз. — ISBN 978-5-369-01682-4 (РИОР). — Текст : непосредственный.

114. Уголовное право России : учебник : для студентов высших учебных заведений, обучающихся по направлению подготовки «Юриспруденция», специальностям «Юриспруденция», «Правоохранительная деятельность» : в 2 томах / [Абдульманов А. А., Борисов С. В., Боровиков В. Б. и др.] ; под редакцией доктора юридических наук, профессора Н. Г. Кадникова. — Москва : Юриспруденция, 2018. — ISBN 978-5-9516-0810-9. — Текст : непосредственный.

115. Уголовно-юрисдикционная деятельность в условиях цифровизации : монография / Н. А. Голованова, А. А. Гравина, О. А. Зайцев и др. ; Институт законодательства и сравнительного правоведения при Правительстве РФ. — Москва : КОНТРАКТ, 2019. — 212 с. — 500 экз. — ISBN 978-5-6041897-2-6. — Текст : непосредственный.

116. **Brenner, S. W.** Cybercrime and the law: challenges, issues and outcomes / S. W. Brenner. — Boston : Northeastern University press, 2012. — 263 p.

117. **Qianyun Wang**. A comparative study of cybercrime in criminal law: China, US, England, Singapore and the Council of Europe. — Rotterdam, 2016. — 381 p.

118. **Heymann, Stephe P.** Legislating computer crime / S. P. Heymann. — Harv. J. On Legis, 1997 (373).

Статьи в периодических изданиях, материалы конференций

119. **Архипов, В. П.** К вопросу о необходимости специальной нормы, предусматривающей уголовную ответственность за мошенничество при получении выплат / В. П Архипов. — Текст : непосредственный // Вестник Томского государственного университета. — 2013. — № 377. — С. 95–98.

120. **Баймолдина, С. М**. Обеспечение информационной безопасности уголовно-правовыми мерами в Республике Казахстан / С. М. Баймолдина. — Текст : непосредственный // Обеспечение национальной безопасности – приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики : сборник статей по материалам XI Российского Конгресса уголовного права, посвященного памяти доктора юридических наук, профессора Владимира Сергеевича Комиссарова (Москва, 31 мая–1 июня 2018 года). — Москва, 2018. — С. 602–608.

121. **Барков, А. В**. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур / А. В. Барков, А. С. Киселев. — Текст :

непосредственный // Банковское право. — 2022. — № 4. — С. 20–27.

122. **Бегишев, И. Р.** Безопасность критической информационной инфраструктуры Российской Федерации / И. Р. Бегишев. — Текст : электронный // Безопасность бизнеса. — 2019. — № 1. — С. 27–32. — URL: www.consultant.ru (дата обращения: 20.10.2021).

123. **Бегишев, И. Р.** Сравнительно-правовой анализ законодательства Великобритании и России в области противодействия преступлениям в цифровой сфере / И. Р. Бегишев, З. И. Хисамова. — Текст : электронный // Электронный научный журнал Байкальского государственного университета. — 2019. — № 3. — URL: www.aljournal.net (дата обращения: 08.02.2023).

Бражник, С. Д. Неправомерное воздействие на критическую информационную инфраструктуру России: дискуссионные вопросы регламентации и толкования квалифицирующего признака, характеризующего тяжкие последствия / С. Д. Бражник, А. А. Чавгун. — Текст : непосредственный // Сборник материалов XV Международной научно-практической конференции «Наука, образование, общество: тенденции и перспективы развития» (Чебоксары, 16 августа 2019 года). — Чебоксары : Интерактив плюс, 2019. — С. 139–141.

124. **Бриллиантов, А. В.** О направлениях совершенствования уголовного закона / А. В. Бриллиантов — Текст : непосредственный // Библиотека уголовного права и криминологии. — 2017. — № 4 (22). — С. 7–13.

125. **Букалерова, Л. А.** К вопросу о значении искусственного интеллекта в уголовном праве / Л. А. Букалерова, Т. Н. Уторова, Д. О. Сизов. — DOI 10.24411/2686-9764-2020-00011– 2020. — Текст : электронный // Пенитенциарная наука : научно-практический журнал. — 2020. — Т. 14. — № 1. — С. 70–75. — Библиогр. : с. 74–75. — URL: www.cyberleninka (дата обращения: 26.05.2022).

126. **Букалерова, Л. А.** О необходимости усиления правовой охраны оборота электронной подписи: современные проблемы теории и практики / Л. А. Букалерова, Р. В. Шагиева. — Текст : непосредственный // Ученые труды Российской академии адвокатуры и нотариата. — 2011. — № 2 (21). — С. 119–124.

127. **Волеводз, А. Г.** Уголовное законодательство об ответственности за компьютерные преступления: опыт разных стран / А. Г. Волеводз, Д. А. Волеводз — Текст : электронный // Правовые вопросы связи. — 2004. — № 1. — С. 37–48. — URL: www.mgimo.ru (дата обращения: 16.11.2022).

128. **Голованова, Н. А.** Новые формы онлайн-преступности за рубежом / Н. А. Голованова. — DOI 10.12737fjflcl.2019.3.4. — Текст : электронный // Журнал зарубежного законодательства и сравнительного правоведения. — 2019. — № 3. — С. 42–57. — Библиогр. : с. 54–57. — URL: www.cyberleninka (дата обращения: 16.12.2022).

129. **Голуб, В. А.** Проблема корректного определения термина «вредоносная программа» / В. А. Голуб, М. В. Овчинникова. — Текст : электронный // Вестник Воронежского государственного университета. — Серия: Системный анализ и информационные технологии. — 2008. — № 1. — С. 138–141. — Библиогр. : с. 141 (10 назв.). — URL: www.vestnik.vsu.ru (дата обращения: 14.08.2022).

130. **Грачева, Ю. В.** Предупреждение девиаций в цифровом мире уголовно-правовыми средствами / Ю. В. Грачева, С. В. Маликов, А. И. Чучаев. — Текст : непосредственный // Право. Журнал Высшей школы экономики. — 2020. — № 1. — С. 188–210. — Библиогр. : с. 208.

131. **Гребенкин, Ф. Б.** Формулирование законодателем составов компьютерных преступлений / Ф. Б. Гребенкин, Л. А. Коврижных. — Текст : непосредственный. // Материалы XV Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (Москва, 25–26 января 2018 года). — Москва, 2018. — С. 627–630.

132. **Дворянсков, И. В.** Виртуально организованная молодежная преступность / И. В. Дворянсков, Е. Е. Панфилов. — Текст : непосредственный // Обеспечение национальной безопасности – приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики : сборник статей по материалам XI Российского Конгресса уголовного права, посвященного памяти доктора юридических наук, профессора Владимира Сергеевича

Комиссарова (Москва, 31 мая–1 июня 2018 года). — Москва, 2018. — С. 355–359.

133. **Дмитренко, А. П.** О нетипичных аспектах соучастия в преступлениях, совершаемых с использованием информационно-коммуникационных технологий / А. П. Дмитренко, Е. А. Русскевич. — Текст : непосредственный // Вестник Академии Генеральной прокуратуры Российской Федерации. — 2017. — № 5 (61). — С. 18–22. — Библиогр. : с. 22.

134. **Дремлюга, Р. И.** Критическая инфраструктура как предмет преступного посягательства / Р. И. Дремлюга, С. С. Зотов, В. Ю. Павлинская. — DOI dx.doi.org/10.24866/1813-3274/2019-2/130-139/ — Текст : электронный // Азиатско-тихоокеанский регион: экономика, политика, право. — 2019. — № 2. — С. 130–139. — Библиогр. : с. 137–139. — URL: www.cyberleninka.ru (дата обращения: 22.11.2022).

135. **Духвалов, А. П.** «Лаборатория Касперского» создает свою операционную систему / А. П. Духвалов. — Текст : электронный. — eLIBRARY ID: 22262517 // Право и кибербезопасность. — 2012. — № 1. — С. 41–47. — URL: http://elibrary.ru (дата обращения: 24.09.2021).

136. **Евдокимов, К. Н.** Актуальные вопросы противодействия компьютерной преступности в Российской Федерации (криминологическое исследование) / Л. Н. Евдокимов. — Текст : непосредственный // Российский следователь. — 2018. — № 10. — С. 56–61. — ISSN: 1812-3783.

137. **Ефремова, М. А.** К вопросу о понятии компьютерной информации / М. А. Ефремова — Текст : электронный // Российская юстиция. — 2012. — № 7. — С. 50–52. — URL: www.justicemag.ru (дата обращения: 16.11.2021).

138. **Ефремова, М. А.** Обеспечение информационной безопасности как одно из направлений уголовной политики / М. А. Ефремова — Текст : непосредственный // Обеспечение национальной безопасности – приоритетное направление уголовно-правовой, криминологической и уголовно-исполнительной политики : сборник статей по материалам XI Российского Конгресса уголовного права, посвященного памяти доктора юридических наук, профессора Владимира Сергеевича Комиссарова (Москва, 31 мая–1 июня 2018

года). — Москва, 2018. — С. 82–86.

139. **Ефремова, М. А.** Уголовно-правовые средства обеспечения информационной безопасности / М. А. Ефремова. — Текст : непосредственный // Материалы XV Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (Москва, 25–26 января 2018 года). — Москва, 2018. — С. 613–617.

140. **Ефремова, М. А.** Уголовно-правовые средства противодействия кибертерроризму / М. А. Ефремова. — Текст : непосредственный // Материалы XVII Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (Москва, 23–24 января 2020 года). — Москва : РГ-Пресс, 2020. — С. 150–154.

141. **Ефремова, М. А.** Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации / М. А. Ефремова. — DOI 10.37973/KUI.2022.10.11.011. — Текст : электронный // Вестник Казанского юридического института МВД России. — 2022. — № 4 (50). — С. 86–92. — URL: www.cyberleninka.ru (дата обращения: 12.02.2023).

142. **Жалинский, А. Э.** Оценка общественной опасности деяния в процессе уголовного правотворчества / А. Э. Жалинский. — Текст : непосредственный // Материалы VI Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (Москва, 29–30 января 2009 года). — Москва : Проспект, 2009. — С. 48–52.

143. **Жарова, А. К.** Правовое регулирование отношений в области предотвращения возможных уязвимостей в информационных технологиях / А. К. Жарова. — DOI 10.18572/2072-3644-2022-1-19-26/ — Текст : электронный // Безопасность бизнеса. — 2022. — № 1. — С. 19–26. — URL: www.old.lawinfo.ru (дата обращения: 10.02.2023).

144. **Жестеров, П. В.** Четвертая промышленная революция: трансформация содержания уголовной репрессии / П. В. Жетеров. — Текст : непосредственный // Материалы XV Международной научно-практической

конференции «Уголовное право: стратегия развития в XXI веке» (Москва, 25–26 января 2018 года). — Москва, 2018. — С. 625–626. — ISBN: 978-5-9988-0588-2.

145. **Ильяшенко, А. Н.** Уголовно-правовая охрана государственных информационных ресурсов по законодательству зарубежных стран / А. Н. Ильяшенко, А. С. Горлов. — Текст : электронный // Общество и право. — 2013. — № 4 (46). — С. 59–63. — Библиогр. : с. 63. — URL: www.cyberleninka.ru (дата обращения: 11.11.2022).

146. **Карабанова, Е. Н.** Понятие объекта преступления в современном уголовном праве / Е. Н. Крабанова. — Текст : непосредственный // Журнал российского права. — 2018. — № 6. — С. 69–77. — Библиогр. : с. 77.

147. **Каримов, В. Х.** Актуальные вопросы борьбы с преступлениями, совершаемыми с использованием систем анонимизации пользователей в сети «Интернет» / В. Х. Каримов. — Текст : непосредственный. — eLIBRARY ID: 35049607 // Российский следователь. — 2018. – № 6. — С. 51–54. — ISSN 1812-3783.

148. **Комаров, А. А.** Отдельное мнение относительно законопроекта «О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации / А. А. Комаров. — Текст : электронный // Вестник Северо-Кавказского гуманитарного института. — 2017. — № 3 (23). — С. 155–160. — URL: www.rusneb.ru (дата обращения: 10.10.2022).

149. **Кондратьев, Ю. А.** Особенности толкования термина «компьютерные технологии» для целей уголовно-правового регулирования / Ю. А. Кондратьев, О. М. Сафонов. — Текст : непосредственный // Конвенционные начала в уголовном праве : материалы Международной научно-практической конференции (Москва, 22 ноября 2013 г.). — Москва : РПА Минюста России, 2014. — ISBN 978-5-89172-715-1 — С. 156–170.

150. **Коротков, А. В.** Безопасность критических информационных инфраструктур в международном уголовном праве / А. В. Коротков, Е. С. Зиновьева. — Текст : непосредственный // Вестник МГИМО-Университета. — 2011. — № 4 (19). — С. 154–162.

151. **Кругликов, Л. Л.** Тяжкие последствия в уголовном праве: объективные и субъективные признаки / Л. Л. Кругликов. — Текст : непосредственный // Уголовное право. — 2010. — № 5. — С. 38–46.

152. **Кругликов, Л. Л.** Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в системе экономической и информационной безопасности государства / Л. Л. Кругликов, О. Г. Соловьев, С. Д. Бражник. — Текст : электронный // Вестник ЯрГУ. — Серия: Гуманитарные науки. — 2019. — № 4. (50). — С. 49–52. — URL: http://j.uniyar.ru (дата обращения: 16.12.2021).

153. **Кругликов, Л. Л**. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ): некоторые проблемы определения признаков состава преступления / Л. Л. Кругликов, С. Д. Бражник, И. А. Пилясов. — Текст : электронный // Журнал юридических исследований. — 2019. — Т. 4. — № 3. — С. 53–62. — URL: http://naukaru.ru (дата обращения: 22.01.2022).

154. **Лапунин, М. М.** Уголовная ответственность за неправомерный доступ к компьютерной информации: общая характеристика и некоторые проблемы квалификации / М. М. Лапунин. — Текст : непосредственный. // Библиотека криминалиста. — ISSN: 2224-0543 — 2013. — № 5 (10). — С. 23–33.

155. **Ларина, Л. Ю.** Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру России / Л. Ю. Ларина. — Текст : электронный // Актуальные вопросы борьбы с преступлениями. — 2017. — № 3. — С. 22–25. — URL: http://istina.msu.ru (дата обращения: 29.09.2021).

156. **Лебедев, С. Я.** Перспективы модернизации уголовного закона как средства обеспечения безопасного развития цифровой экономики / С. Я. Лебедев.

— Текст : непосредственный // Криминологические основы уголовного права : материалы XI Российского конгресса уголовного права (Москва, 31 мая–1 июня 2018 г.), посвященного памяти доктора юридических наук, профессора Владимира Сергеевича Комиссарова. — Москва : Юрлитинформ, 2018. — С. 155–159.

157. **Летелкин, Н. В.** К вопросу об определении понятия преступлений, совершаемых с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») / Н. В. Летелкин. — Текст : непосредственный // Уголовное право: стратегия развития в XXI веке : материалы XV Международной научно-практической конференции (Москва, 25—26 января 2018 г.). — Москва : Проспект, 2018. — С. 617–619.

158. **Лисаченко, А. В.** Право виртуальных миров: новые объекты гражданских прав / А. В. Лисаченко. — Текст : электронный // Российский юридический журнал. — Екатеринбург : Изд-во УрГЮА, 2014. — № 2 (25). — С. 104–110. — URL: www.consultant.ru (дата обращения: 20.03.2022).

159. **Лопатина, Т. М.** Трансформация уголовного права и уголовного процесса в условиях развития цифровых технологий: на примере использования специальных технических средств, предназначенных для негласного получения информации / Т. М. Лопатина. — Текст : непосредственный. // Библиотека криминалиста. Научный журнал. — 2018. — № 3 (38). — С. 64–69.

160. **Лузянин, С. Г**. Особенности правового регулирования борьбы с преступностью в Китае / С. Г. Лузянин, П. В. Трощинский, Я. А. Суходолов. — DOI 10.18572/2072-3644-2022-1-19-26. — Текст : непосредственный // Всероссийский криминологический журнал. — 2016. — Т. 10. — № 4. — С. 812–824. — Библиогр. : с. 822–824.

161. **Мелешко, Д. А.** «Инструментальный» характер компьютерных преступлений и его влияние на квалификацию / Д. А. Мелешко, Д. О. Чернявский, Г. А. Шарафетдинова. — Текст : непосредственный // Законность. — 2020. — № 3. — С. 55–57.

162. **Минин, А. Я.** Кибербезопасность и защита информационных систем

/ А. Я. Минин. — Текст : электронный // Право и кибербезопасность. — Москва : Юрист, 2013. — № 2 (3). — С. 28–35. — URL: www.lawbrary.ru (дата обращения: 17.04.2022).

163. **Молчанов, Н. А.** Концептуально-политический и формально-юридический анализ Парижского призыва к доверию и безопасности в киберпространстве и российские инициативы в области международного права / Н. А. Молчанов, Е. К. Матевосова. — DOI 10.17803/1994-1471.2020.110.1.133-141. — Текст : электронный // Актуальные проблемы российского права. — 2020. — № 1. — С. 133–141. — Библиогр. : с. 141 (5 назв.). — URL: www.cyberleninka.ru (дата обращения: 12.07.2022).

164. **Мысина, А. И.** К вопросу о региональных правовых основах сотрудничества государств по противодействию преступлениям в сфере информационных технологий / А. И. Мысина. — Текст : электронный // Российская юстиция. — 2019. — № 5. — С. 20–24. — URL: www.yusticemag.ru (дата обращения: 16.11.2022).

165. **Новичков, В. Е.** Социально-правовое обоснование введения уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации / В. Е. Новичков, И. Г. Пыхтин. — DOI 10.24411/1999-6241-2018.12004. — Текст : электронный // Психопедагогика в правоохранительных органах. — 2018. — № 2 (73). — С. 25–29. — Библиогр. : с. 28–29 (11 назв.). — URL: www.cyberleninka.ru (дата обращения: 24.12.2022).

166. **Поветкина, Н. А.** Правовая форма интеграции информационных систем и информационных технологий в сферу публичных финансов / Н. А. Поветкина. — Текст : непосредственный // Журнал российского права. — 2018. — № 5. — С. 96–112. — Библиогр. : с. 112 (5 назв.).

167. **Простосердов, М. А**. Дефекты санкций основных и квалифицированных составов преступлений Особенной части УК РФ / М. А. Простосердов. — Текст : непосредственный // Российское правосудие. — 2020. — № 08 (172). — С. 99–104. — Библиогр. : с. 104 (5 назв.).

168. **Пыхтин, И. Г.** Обеспечение уголовно-правовой охраны национальных объектов критической информационной инфраструктуры Германии, Австрии, Швейцарии и Франции / И. Г. Пыхтин. — Текст : электронный // Известия Юго-Западного государственного университета. — Серия : История и право. — 2019. — Том 9. —№ 2 (31). — С. 108–115. — Библиогр. : с. 113–114 (20 назв.). — URL: www.swsu.ru (дата обращения: 24.10.2022).

169. **Пыхтин, И. Г.** Логико-языковые феномены, аккумулирующие в своих значениях предмет состава неправомерного воздействия на критическую информационную инфраструктуры России (ст. 274.1 УК РФ) / И. Г. Пыхтин. — DOI https://doi.org/10.17308/vsu.proc.law.2021.1/3295. — Текст : электронный // Вестник ВГУ. — Серия : Право. — 2021. — № 1. — С. 189–297. — URL: www.cyberleninka.ru (дата обращения: 26.03.2022).

170. **Решетников, А. Ю.** Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК России) / А. Ю. Решетников, Е. А. Русскевич. — Текст : непосредственный // Законы России: опыт, анализ, практика. — 2018. — № 2 (66). — С. 51–55.

171. **Решетников, А. Ю.** Конструкция состава преступления и ее влияние на установление момента его окончания / А. Ю. Решетников, Л. А. Букалерова. — Текст : непосредственный // Уголовное наказание в России и за рубежом: проблемы назначения и исполнения (к 10-летию принятия Европейских пенитенциарных правил) : сборник материалов Международной научно-практической конференции (Вологда, 11 ноября 2016 года) : в 2 частях. — Часть 1 / под общей редакцией П. В. Голодова. — Вологда, 2017. — С. 249–251.

172. **Решняк, М. Г.** О некоторых вопросах современного уголовно-правового законотворчества / М. Г. Решняк. — Текст : непосредственный // Российский следователь. — 2014. — № 3. — С. 25–28.

173. **Рогова, Е. В.** Правила построения квалифицирующих и привилегирующих признаков состава преступления / Е. В. Рогова. — Текст :

непосредственный // Пробелы в российском законодательстве. — 2013. — № 5. — С. 172–178.

174. **Русскевич, Е. А.** Уголовное право и информатизация / Е. А. Русскевич. — Текст : непосредственный // Журнал российского права. — 2017. — № 8. — С. 73–80. — Библиогр. : с. 79–80 (20 назв.).

175. **Русскевич, Е. А.** Законодательные подходы к криминализации деяний, связанных с неправомерным доступом к компьютерной информации в странах Содружества Независимых Государств / Е. А. Русскевич. — DOI 10.13727/art.2018.1.16. — Текст : непосредственный // Журнал зарубежного законодательства и сравнительного правоведения. — 2018. — № 1. — С. 116–121. — Библиогр. : с. 121 (7 назв.).

176. **Русскевич, Е. А.** Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации / Е. А. Русскевич, А. Ю. Решетников. — Текст : непосредственный // Уголовное право. — 2018. — № 2. — С. 86–95.

177. **Русскевич, Е. А.** Международно-правовые подходы противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий / Е. А. Русскевич. —Текст : непосредственный // Международное уголовное право и международная юстиция. — 2018. — № 3. — С. 10–13.

178. **Русскевич, Е. А.** Уголовная ответственность за преступления в сфере компьютерной информации по законодательству Китайской Народной Республики: сравнительно-правовой анализ / Е. А. Русскевич. — DOI 10.12737/art.2018.5.15. — Текст : непосредственный // Журнал зарубежного законодательства и сравнительного правоведения. — 2018. — № 5. — С. 108–113. — Библиогр. : с. 113 (13 назв.).

179. **Русскевич, Е. А.** Об отдельных проблемах квалификации создания, использования и распространения вредоносных компьютерных программ / Е. А. Русскевич, А. С. Мельников. — Текст : непосредственный // Российский следователь. — 2018. — № 8. — С. 60–64.

180. **Русскевич, Е. А.** О квалификации преступлений в сфере компьютерной информации, совершаемых с использованием служебного положения / Е. А. Русскевич. — Текст : непосредственный // Российское правосудие. — 2019. — № 2. — С. 35–41.

181. **Русскевич, Е. А.** О совершенствовании уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации / Е. А. Русскевич. Текст : непосредственный // Уголовное право: стратегия развития в XXI веке : материалы XVIII Международной научно-практической конференции «Уголовное право: стратегия развития в XXI веке» (Москва, МГЮА им. О. Е. Кутафина, 21–22 января 2021 г.). — М. : РГ-Пресс, 2021. — С. 187–190.

182. **Русскевич, Е. А.** Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / Е. А. Русскевич, И. Г. Чекунов. — Текст : непосредственный // Уголовное право. — 2022. — № 5. — С. 26–35.

183. **Савенков, А. Н.** Противодействие киберпреступности в финансово кредитной сфере как вектор обеспечения глобальной безопасности / А. Н. Савенков. — Текст : непосредственный // Государство и право. — 2017. — № 10. — С. 5–18.

184. **Серебренникова, А. В.** Правовые основы кибербезопасности в Российской Федерации / А. В. Серебренникова — Текст : непосредственный // Пробелы в российском законодательстве. — 2021. — № 4. — С. 260 – 265.

185. **Серебренникова, А. В.** Преступления в сфере цифровых технологий в законодательстве России и зарубежных стран : постановка проблемы / А. В. Серебренникова — Текст : непосредственный // Кризисы мировой науки и техники : парадигмы дальнейшего развития. Материалы I Международной научно-практической конференции (20 апреля 2020 г.). — Ростов-на-Дону : Издательство Южного университета ИУБиП, 2020. — С. 62 – 67.

186. **Степанов-Егиянц, В. Г.** Критическая информационная инфраструктура России: понятие и вопросы уголовно-правовой охраны / В. Г. Степанов-Егиянц — Текст : электронный // Евразийский юридический журнал. —

2019. — № 2 (129). — С. 265–268. — Библиогр. : с. 268 (15 назв.). — URL: http://crimesceince.ru (дата обращения: 12.11.2021).

187. **Соловьев, В. С**. Уголовно-правовая оценка киберпреступлений: что имел в виду законодатель? / В. С. Соловьев. — Текст : непосредственный // Уголовное право: стратегия развития в XXI веке : материалы XV Международной научно-практической конференции (Москва, 25–26 января 2018 г.). — Москва : Проспект, 2018. — С. 619–623.

188. **Тирранен, В. А.** Проблема уголовной ответственности за крипто-вирусные атаки. — Текст : непосредственный // Уголовное право: стратегия развития в XXI веке : материалы XV Международной научно-практической конференции (Москва, 25–26 января 2018 г.). — Москва, 2018. — С. 637–640.

189. **Тропина, Т. Л.** Борьба с киберпреступностью: возможна ли разработка универсального механизма? / Т. Л. Тропина. — Текст электронный // Международное правосудие. — 2012. — № 3. — С. 86–95. — URL: www.cyberleninka.ru (дата обращения: 05.10.2021).

190. **Трунцевский, Ю. В.** Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов / Ю. В. Трунцевский. — Текст непосредственный // Журнал российского права. — 2019. — № 5. — С. 99–106. — Библиогр. : с. 106 (7 назв.)

191. **Хабриева, Т. Я.** Право в условиях цифровой реальности / Т. Я. Хабриева, Н. Н. Черногор. — Текст непосредственный // Журнал российского права. — 2018. — № 1. — С. 85–102. — Библиогр. : с. 102 (17 назв.)

192. Цифровизация рыночных отношений: вопросы экономики и права: сборник научных статей Всероссийской научно-практической конференции (Москва, 20 июня 2022 г.) / Ответственный редактор доктор юридических наук, профессор, заслуженный юрист РФ Б. В. Яцеленко. — Москва : Проспект, 2022. — 182 с. — Текст : непосредственный.

193. **Armin, J.** Cybercrime Economic Costs: No Measure No Solution / J. Armin, B. Thompson, D. Ariu, G. Giacinto, F. Roli // Paper presented at 10th International Conference on Availability, Reliability and Security. — 2015. — P. 701–

710.

194. **Bushra Mohamed.** Cyber Crime in Kingdom of Saudi Arabia: The Threat Today and the Expected Future / Bushra Mohamed // Information and Knowledge Management. — 2013. — № 12. — P. 132–148. — Текст : электронный. — URL: https://www.researchgate.net/publication/309040131_Cyber_Crime_in_Kingdom_of_Saudi_Arabia_The_Threat_Today_and_the_Expected_Future (дата обращения: 04.02.2023).

195. **Chen, L.** The discussion on computer crime and its legislation / L. Chen // Legal science. — 1990. — № 1. — P. 42–44.

196. **Clough, J. A**. World of Difference: The Budapest Convention on Cybercrime and the Challenges of Harmonisation / J. A. Clough // Monash University Law Review. — 2015. — № 40 (3). — P. 698–736.

197. **Decker, C.** Cyber-crime 2.0: An argument to update the United States criminal code to reflect the changing nature of cyber-crime / C. Decker // USA University Southern California. — 2008. — № 81 (5). — P. 972–995.

198. **Li, Huaisheng**. The evolution of cybercrime in three generations of the information network and the law-making / Li Huaisheng // Legal forum. — 2015. — № 4.

199. **Mele, Stefano.** Legal consideration on cyber-weapons and their definition / S. Mele // Journal of Law & Cyber Warfare. — 2014. — Volume 3. — Issue 1. — P. 53–69.

200. **Putman, T.** International Responses to Cyber Crime / T. Putman & D. Elliott // S. Goodman and A. Sofaer (Eds.). The Transnational Dimension of Cyber Crime and Terrorism. — Stanford : Hoover Institution Press, 2001. — P. 35–69.

201. **Rhaman, M.** Cyberspace Claiming New Dynamism in the Jurisprudential Philosophy: A Substantive Analysis of Conceptual and Institutional Innovation / M. Rhaman, M. Khan, Mohammad, M. N.&Rhaman // International Journal of Law and Management. — 2009. — № 51 (5). — P. 274–290.

202. **Viano, E.** Cybercrime: Definition, Typology and Criminalisation / E. Viano // Cybercrime, Organised Crime, and Societal Responses: International

Approaches, 2016. — P. 3–23.

Диссертации, авторефераты диссертаций

203. **Айсанов, Р. М.** Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Айсанов Руслан Мухамедович ; Российская академия правосудия. — Москва, 2006. — 31 с. — Текст : непосредственный.

204. **Бегишев, И. Р.** Понятие и виды преступлений в сфере обращения цифровой информации : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Бегишев Ильдар Рустамович. — Казань, 2017. — 30 с. — Место защиты : Казанский (Приволжский) федеральный университет. — Текст : непосредственный.

205. **Букалерова, Л. А.** Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени доктора юридических наук / Букалерова Людмила Александровна. — Москва, 2007. — 574 с. — Место защиты : Московский государственный университет им. М. В. Ломоносова. — Текст : непосредственный.

206. **Васильевский, А. В**. Дифференциация уголовной ответственности и наказания в Общей части уголовного права : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени кандидата юридических наук / Васильевский Александр Валентинович. — Ярославль, 2000. — 219 с. — Библиогр. : с. 4. —

Текст : непосредственный.

207. **Гаджиев, М. С.** Криминологический анализ преступности в сфере компьютерной информации (по материалам Республики Дагестан) : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Гаджиев Марат Салахетдинович. — Махачкала, 2004. — 21 с. — Текст : непосредственный.

208. **Грибов, А. С.** Дифференциация ответственности за экономические преступления в России, ФРГ и США: сравнительно-правовое исследование : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Грибов Александр Сергеевич. —Ярославль, 2011. — 26 с. — Текст : непосредственный.

209. **Ефремова, М. А.** Уголовно-правовая охрана информационной безопасности : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени доктора юридических наук / Ефремова Марина Александровна. — Москва, 2018. — 427 с. — Место защиты : Академия Генеральной прокуратуры РФ. — Текст : непосредственный.

210. **Кабанова, А. Ж.** Преступления в сфере компьютерной информации: уголовно-правовые и криминологические аспекты : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Кабанова Анна Жунусовна. — Ростов-на-Дону, 2004. — 28 с. — Текст : непосредственный.

211. **Лесниевски-Костарева, Т. А.** Дифференциация уголовной ответственности : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени доктора юридических наук / Лесниевски-Костарева Татьяна Александровна. — Москва, 1998. — 493с. — Библиогр. : с. 52. — Текст : непосредственный.

212. **Малышенко, Д. Г.** Уголовная ответственность за неправомерный доступ к компьютерной информации : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Малышенко Дмитрий Геннадьевич ; Юридический институт МВД России. — Текст : непосредственный — Москва, 2002. — 24 с.

213. **Рогова, Е. В.** Учение о дифференциации уголовной ответственности : : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени доктора юридических наук / Рогова Евгения Викторовна. — Москва, 2014. — 596 с. — Библиогр. : с. 170. — Библиогр. : с. 170. — Место защиты : Академия управления МВД России. — Текст : непосредственный.

214. **Русскевич, Е. А.** Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени доктора юридических наук / Русскевич Евгений Александрович. — Москва, 2020. — 521 с. — Библиогр. : с. 323. — Место защиты : Университет МВД России имени В. Я. Кикотя. — Текст : электронный // Электронная библиотека диссертаций. — URL: https://diss.rsl.ru/?lang=ru (дата обращения: 15.07.2022).

215. **Чекунов, И. Г.** Криминологическое и уголовно-правовое обеспечение предупреждения киберпреступности : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : автореферат диссертации на соискание ученой степени кандидата юридических наук / Чекунов Игорь Геннадбевич. — Москва, 2013. — 23 с. — Место защиты : Московский университет МВД России. — Текст : электронный // Электронная библиотека диссертаций. — URL: — URL: https://diss.rsl.ru/?lang=ru (дата обращения: 12.07.2022).

216. **Чупрова, А. Ю.** Уголовно-правовые механизмы регулирования

отношений в сфере электронной коммерции : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени доктора юридических наук / Чупрова Антонина Юрьевна. — Москва, 2015. — 608 с. — Место защиты : Российская правовая академия Минюста России. — Текст : электронный // Электронная библиотека диссертаций. — URL: https://diss.rsl.ru/?lang=ru (дата обращения: 30.07.2021).

217. **Шахрай, С. С.** Система преступлений в сфере компьютерной информации: сравнительно-правовой, социолого-криминологический и уголовно-правовой аспекты : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени кандидата юридических наук / Шахрай Сергей Сергеевич. — Москва, 2010. — 214 с.— Место защиты : Академия экономической безопасности МВД России. — Текст : электронный // Электронная библиотека диссертаций. — URL: https://diss.rsl.ru/?lang=ru (дата обращения: 03.08.2021).

Иные публикации и интернет-ресурсы

218. В Сбербанке рассчитали долю совершенных детьми киберпреступлений. — Текст : электронный // Группа компаний «РБК». — URL: https://www.rbc.ru/society/04/07/2018/5b3ceb009a7947b19e91997e (дата публикации: 04.07.2018 ; дата обращения: 15.05.2022).

219. Власти Венесуэлы установили причастных к атакам на энергосистему. — Текст : электронный // РИА Новости. — URL: https://ria.ru (дата публикации: 24.04.2019 ; дата обращения: 15.04.2022).

220. **Федуненко, Е.** Кибератаки на ядерные объекты: история вопроса / Е. Федуненко, Е. Чернышева. — Текст : электронный // Газета «Коммерсантъ». — URL: www.kommersant.ru (дата публикации: 20.01.2017 ; дата обращения: 10.04.2022).

221. **Федотенков, С.** 10 самых впечатляющих кибератак в истории / С. Федотенков. — Текст : электронный. — URL: https://3dnews (дата публикации:

30.05.2020 ; дата обращения: 15.04.2022).

222. **Черненко, Е.** Хакеры смерти. Россию обвиняют в очередной кибератаке, на сей раз – с летальным исходом / Е. Черненко, П. Цуканов. — Текст : электронный // Газета «Коммерсантъ». — URL: www.kommersant.ru (дата публикации: 28.09.2020 ; дата обращения: 19.12.2020).

223. Computer-Related Crime: Analysis of Legal Polici. — Paris: OECD, 1986. — Текст : электронный. — URL: http://www.unicri.it/services/library_documentation/catalogue_ (дата обращения: 11.10.2022).

224. Cyber crime & cyber security: Trends in Africa (96 p.) — Текст : электронный. — URL: www.thegfce.org, Publiched November, 2016 (дата обращения: 08.02.2023).

225. Верховный Суд Российской Федерации : официальный сайт. — URL: http://www.vsrf.ru

226. Газета.Ру : [сайт] / учредитель АО «Газета.Ру». — Москва, 1999 . — Обновляется в течение суток. — URL: https://www.gazeta.ru

227. Генеральная прокуратура Российской Федерации : Официальный сайт. — URL: www.epp.genproc.gov.ru

228. Единый реестр правовых актов и других документов СНГ. URL: http://cis.minsk.by

229. Министерство внутренних дел Российской Федерации : Официальный сайт. — URL: https://мвд.рф

230. Организация Объединенных Наций : официальный сайт. — URL: www.un.org

231. Официальный портал судов общей юрисдикции города Москвы. — URL: www.mos-gorsud.ru

232. Правительство Российской Федерации : официальный сайт. — Москва. — Обновляется в течение суток. — URL: http://governmtnt.ru

233. Президент Российской Федерации : официальный сайт. — Москва. — Обновляется в течение суток. — URL: http://kremlin.ru

234. Российское информационное агентство (РИА Новости) :

официальный сайт. — URL: https://ria.ru

235. Следственный комитет Российской Федерации : официальный сайт. — Москва. — Обновляется в течение суток. — URL: www.sledcom.ru

236. Справочно-правовая система «Гарант». — URL: www.garant.ru

237. Справочно-правовая система «КонсультантПлюс». — URL: www.consultant.ru

238. Судебный департамент при Верховном Суде Российской Федерации : официальный сайт. — Москва. — URL: www.cdep.ru

239. Судебные и нормативные акты РФ : электронная база данных. — URL: www.sudact.ru

240. Судебные решения РФ : электронная база данных. — URL: www.судебныерешения.рф

241. ФКУ «ГИАЦ МВД России» : официальный сайт. — URL: www.мвд.рф

242. Электронная база данных системы «Гарант» www.base.garant.ru

243. Электронная библиотека : библиотека диссертаций : сайт / Российская государственная библиотека. — Москва : РГБ, 2003 –. — URL: https://diss.rsl.ru/?lang=ru — Режим доступа для зарегистрир. читателей РГБ.

244. Электронный фонд правовых и нормативно-технических документов. — URL: www.docs.cntd.ru

245. eLIBRARY.RU : научная электронная библиотека : сайт. — Москва, 2000 – . — URL: http://elibrary.ru — Режим доступа для зарегистрир. пользователей.

Приложение А

(рекомендуемое)

ПОСТАНОВЛЕНИЕ

Пленума Верховного Суда Российской Федерации

(проект)

дата _____ **№ _____**

г. Москва

О внесении изменений в постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 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"»

В связи с имеющимися в судебной практике вопросами Пленум Верховного Суда Российской Федерации, руководствуясь статьей 126 Конституции Российской Федерации, статьями 2 и 5 Федерального конституционного закона от 5 февраля 2014 года № 3-ФКЗ «О Верховном Суде Российской Федерации»,

постановляет

внести изменения в постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 года № 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"».

Пункт 13 изложить в следующей редакции:

«13. Предметом преступления, предусмотренного статьей 274^1 Уголовного кодекса Российской Федерации (далее также — УК РФ), является значимый объект

критической информационной инфраструктуры (независимо от категории значимости), характеризующийся двумя критериями:

1) объективный критерий социальной, политической, экономической, экологической или оборонной (для безопасности государства и правопорядка) значимости (статья 7 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»);

2) формальный критерий, связанный с включением объекта в Реестр значимых объектов критической информационной инфраструктуры (статья 8 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»).

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

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 критической информационной инфраструктуры, не может оцениваться в рамках статьи 274^1 УК РФ и требует квалификации по статье 272 УК РФ. Данным правилом необходимо руководствоваться и при разрешении вопросов об обратной силе уголовного закона.

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 статье 274^1 со ссылкой на часть 3 статьи 30 УК РФ.

Действия лица квалифицируются по части 1 статьи 274^1 УК РФ, если установлено, что компьютерные программы или иная компьютерная информация предназначены для незаконного воздействия именно на критическую информационную инфраструктуру Российской Федерации, определение понятия

которой содержится в статье 2 Федерального закона от 26 июля 2017 года № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В ином случае действия лица при наличии на то оснований могут быть квалифицированы по статье 273 УК РФ.

При этом следует учитывать, что использование вредоносных компьютерных программ для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (в том числе в случае, когда осуществляется распространение этих программ на объекты критической информационной инфраструктуры исключительно для их последующего использования) полностью охватывается частью 2 статьи 274^1 УК РФ и дополнительной квалификации по статье 273 УК РФ не требует.

По смыслу части 2 статьи 274^1 УК РФ под вредом следует понимать:

1) нарушение функционирования объекта критической информационной инфраструктуры;

2) прекращение функционирования объекта критической информационной инфраструктуры;

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

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

5) нарушение безопасности обрабатываемой таким объектом информации.

Председатель Верховного Суда
Российской Федерации В. М. Лебедев

Секретарь Пленума, судья Верховного Суда
Российской Федерации В. В. Момотов

Приложение Б

(справочное)

Результаты анкетирования, проведенного в период с 2018 по 2022 гг. (157 респондентов)

Вопрос	Варианты ответов	% ответив-ших
1. Существует ли в настоящее время объективная необходимость проведения комплексного диссертационного исследования вопросов законодательного определения и квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ст. 274^1 УК РФ)?	а) да	89
	б) нет	5
	в) затрудняюсь ответить	-
	г) Ваш вариант ответа	6
2. Как Вы оцениваете современные процессы цифровизации бизнеса, государственного и муниципального управления?	а) положительно	78
	б) отрицательно	11
	в) нейтрально	5
	д) Ваш вариант ответа	6
3. Поддерживаете ли Вы выделение специальной нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации?	а) поддерживаю	77
	б) не поддерживаю	18
	в) Ваш вариант ответа	5
4. Поддерживаете ли Вы изложение п. 8 ст. 2 Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» в следующей редакции: «субъекты критической информационной инфраструктуры – государственные органы, государственные	а) поддерживаю	64
	б) не поддерживаю	15
	в) затрудняюсь ответить	10
	г) Ваш вариант ответа	1

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»?		
5. Согласны ли Вы, что значимость объекта критической информационной инфраструктуры напрямую влияет на степень общественной опасности совершенного в отношении него неправомерного воздействия. И в этом отношении ст. 274[1] УК РФ требует доработки. При этом все основные составы преступлений, предусмотренных ст. 274[1] УК РФ, будут предполагать совершение посягательства в отношении объектов критической информационной инфраструктуры третьей категории. Дифференциация ответственности будет реализована в зависимости от совершения посягательства на защищенные информационные объекты второй и первой категорий значимости?	а) согласен	84
	б) не согласен	6
	в) Ваш вариант ответа	10
6. Согласны ли Вы, что на современном этапе развития доктрины уголовного права следует признать, что 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?	а) согласен	79
	б) не согласен	10
	в) затрудняюсь ответить	5
	г) Ваш вариант ответа	6

7. Ваше мнение относительно новой редакции ст. 274^1 УК РФ, а также проектируемой 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	а) поддерживаю	74
	б) не поддерживаю	21
	в) затрудняюсь ответить	5
	г) Ваш вариант ответа	-

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 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»		