Оригинальная статья / Original article

https://doi.org/10.21869/2223-1501-2023-13-2-165-176

Актуальные проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации

И. И. Малыгин[1] ✉

[1]Министерство юстиции Российской Федерации
ул. Житная, д. 14, г. Москва 119991, Российская Федерация

✉ e-mail: aspugpravo@yandex.ru

Резюме

Актуальность. *Защита объектов критической информационной инфраструктуры является актуальной задачей обеспечения информационной безопасности государства. Особую значимость данная проблема приобрела в период проведения специальной военной операции на Украине – за это время количество компьютерных атак на отечественную информационную инфраструктуру возросло многократно. На протяжении нескольких лет применение статьи 274.1 Уголовного кодекса Российской Федерации характеризуется последовательным ростом. Изучение судебно-следственной практики свидетельствует о наличии юридико-технических недостатков нормы и проблем, связанных с ее применением.*

Целью *является получение нового научного знания о реализации механизма уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации, обоснование предложений, направленных на преодоление трудностей, возникающих при применении статьи 274.1 Уголовного кодекса Российской Федерации.*

Задачи: *выявить проблемы квалификации неправомерного воздействия на объекты критической информационной инфраструктуры, сформулировать предложения по совершенствованию отечественного уголовного законодательства и правоприменения.*

Методология. *Методологическую базу исследования составляют общенаучные и частнонаучные методы познания действительности, такие как анализ, синтез, индукция, формально-юридический, абстрактно-логический и другие.*

Результаты*. В ходе исследования проанализированы данные судебной статистики, правоприменительная практика по делам о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации, исследованы доктринальные источники и аналитические материалы.*

Выводы. *В работе обоснованы следующие положения: преобладающим направлением реализации статьи 274.1 Уголовного кодекса Российской Федерации является ее применение в случаях нарушения правил эксплуатации средств хранения компьютерной информации работниками компаний, оказывающих услуги в сфере связи (операторов связи); на уровне судебно-следственной практики наблюдается расхождение в толковании общественно опасных последствий в виде вреда объекту критической информационной инфраструктуры Российской Федерации; следует признать ошибочным встречающееся на практике решение о квалификации содеянного по части 1 статьи 274.1 Уголовного кодекса Российской Федерации в некоторых ситуациях.*

Ключевые слова*: преступления; компьютерная информация; особенности квалификации; объект; информационная инфраструктура.*

Конфликт интересов*: Автор декларирует отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Малыгин И. И. Актуальные проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Известия Юго-Западного государственного университета. Серия: История и право. 2023. Т. 13, № 2. С. 165–176. https://doi.org/10.21869/2223-1501-2023-13-2-165-176.

Поступила в редакцию 28.02.2023 Принята к публикации 27.03.2023 Опубликована 28.04.2023

Actual Problems of Qualification of Unlawful Impact on the Critical Information Infrastructure of the Russian Federation

Ivan I. Malygin[1] ✉

[1]Ministry of Justice of the Russian Federation
14 Zhitnaya Str., Moscow 119991, Russian Federation

✉ e-mail: aspugpravo@yandex.ru

Abstract

Relevance. *Protection of objects of critical information infrastructure is an urgent task of ensuring the information security of the state. This problem acquired particular significance during the period of the special military operation in Ukraine - during this time the number of computer attacks on the domestic information infrastructure has increased many times over. For several years, the application of Art. 274.1 of the Criminal Code of the Russian Federation is characterized by consistent growth. The study of judicial and investigative practice indicates the presence of legal and technical shortcomings of the norm and problems associated with its application.*

The ***purpose*** *is to obtain new scientific knowledge about the implementation of the mechanism of criminal law protection of the critical information infrastructure of the Russian Federation, to substantiate proposals aimed at overcoming the difficulties that arise in the application Art. 274.1 of the Criminal Code of the Russian Federation.*

Objectives: *to identify the problems of qualifying unlawful impact on critical information infrastructure facilities, to formulate proposals for improving domestic criminal legislation and law enforcement.*

Methodology. *The methodological base of the research is made up of general scientific and particular scientific methods of cognition of reality, such as analysis, synthesis, induction, formal-legal, abstract-logical and others.*

Results. *The study analyzed data from judicial statistics, law enforcement practice in cases of unlawful impact on the critical information infrastructure of the Russian Federation, studied doctrinal sources and analytical materials.*

Conclusions. *The following provisions are formulated and substantiated in the work: 1) at the moment, the main direction of implementation Art. 274.1 of the Criminal Code of the Russian Federation is its application in cases of violation of the rules for the operation of computer information storage facilities by employees of companies providing services in the field of communications (telecom operators); 2) at the level of judicial and investigative practice, there is a discrepancy in the interpretation of socially dangerous consequences in the form of harm to an object of the critical information infrastructure of the Russian Federation.; 3) it should be recognized as erroneous in practice the decision to qualify the deed under Part 1 of Art. 274.1 of the Criminal Code of the Russian Federation in situations.*

Keywords: *crimes; computer information; qualification features; object; information infrastructure.*

Conflict of interest: *The Author declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Malygin I. I. Actual Problems of Qualification of Unlawful Impact on the Critical Information Infrastructure of the Russian Federation. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law*. 2023; 13(2): 165–176. (In Russ.) https://doi.org/10.21869/2223-1501-2023-13-2-165-176.

Received 28.02.2023 Accepted 27.03.2023 Published 28.04.2023

***

Введение

С каждым днем цифровизация общественной жизни, экономики и государственного управления становится все более всеохватывающим процессом. Обусловлено это преимущественно тем обстоятельством, что 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. 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. В литературе последнего времени данной проблематике уделяется значительное внимание [1; 2; 3; 4; 5; 6].

С 2017 г. в отечественном уголовном законодательстве предусмотрена специальная норма об ответственности за компьютерные атаки и иное неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации (ст. 274.1 УК РФ). В доктрине уголовного права реализация данной законотворческой инициативы в целом была встречена позитивно [7; 8; 9]. Весьма редкое явление в современных условиях. Зачастую научная общественность курс законодателя на казуализацию уголовного закона подвергает критике, справедливо ссылаясь на то обстоятельство, что это приводит к многочисленным сложностям на уровне правоприменения.

В отдельных странах (например, в Китае) само включение компьютерной информации и соответствующей инфраструктуры в сферу уголовно-правовой охраны изначально осуществлялось именно с криминализации посягательств на ресурсы государственных органов и иных наиболее важных (критичных) субъектов. Компьютерная информация физических лиц была поставлена под защиту уголовного закона значительно позднее [10]. Своей спецификой обладает уголовно-правовое противодействие посягательствам на объекты критической информационной инфраструктуры в странах Европейского союза [11].

С момента закрепления норма показала свою востребованность. По данным Министерства внутренних дел Российской Федерации: в 2018 г. было зарегистрировано лишь одно преступление (в Камчатском крае), в 2019 г. – 4, в 2020 г. – 22, в 2021 г. – 159, за 2022 г. зарегистрировано уже 519 преступлений (рост на 226,41%)[1].

В правоприменительной практике возникает множество вопросов относительно толкования признаков 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 Российской Федерации № 37 от 15 декабря 2022 г. «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»[2] данные проблемы не получили своего разрешения.

Методология

Методологическая основа проведенного исследования была построена на традиционном сочетании общенаучных и

[1] По данным ФГКУ «ГИАЦ МВД России».

[2] О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда Российской Федерации № 37 от 15 декабря 2022 г. // Верховный Суд Рос. Федерации: сайт. URL: https://www.vsrf.ru/documents/own/31913/ (дата обращения: 05.02.2023).

специальных методов (анализ, синтез, формально-юридический, абстрактно-логический и др.). Решение поставленных задач осуществлялось посредством изучения научных статей, монографий, учебных и учебно-практических пособий, диссертаций и авторефератов диссертаций по исследуемой проблематике.

Эмпирическая основа работы включает в себя открытые и опубликованные материалы судебной практики, аналитические справки и отчеты государственных органов и служб, обзоры и заключения по кибербезопасности компаний, деятельность которых связана с обеспечением информационной безопасности. Отдельные выводы и положения настоящей работы подкреплены интервьюированием ученых и практиков, в том числе в IT-сфере.

Результаты и их обсуждение

В литературе совершенно справедливо отмечается, что ст. 274.1 УК РФ наследовала практически все противоречия и проблемы, связанные с толкованием конструктивных и квалифицирующих признаков, от общих норм-предшественниц, предусмотренных ст. 272–274 УК РФ [12; 13; 14]. Согласимся с этим. В каком-то смысле такой результат был предсказуем, поскольку само построение ст. 274.1 УК РФ по большому счету было реализовано путем объединения уже имеющихся в главе 28 УК РФ норм с той лишь разницей, что соответствующие действия затрагивают специфический предмет.

В то же время можно уверенно говорить о том, что ст. 274.1 УК РФ присущи и свои специфические особенности. Весьма сложным и до конца не решенным является вопрос о толковании предмета исследуемого преступления, т. е. самого объекта критической информационной инфраструктуры. Здесь в целом сложилось два направления. Первое предполагает, что такими объектами являются не любые информационные системы субъекта критической информационной инфраструктуры, а только значимые и категорированные объекты.

В рамках второго направления этот вопрос решается иначе: объектом критической инфраструктуры должны признаваться все без исключения информационные системы субъекта, независимо от их категорирования и участия в обеспечении критических процессов. Так, по одному из дел представитель ФСТЭК России отмечает, 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].

Однако изучение правоприменительной 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

[1] Апелляционное определение Астраханского областного суда от 14.04.2022 г. № 22-787/2022 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/67736586/ (дата обращения: 05.02.2023).

информационной инфраструктуры. Иная практика единична.

Довольно сомнительной представляется мысль, согласно которой *любая* информационная система крупной компании-субъекта критической информационной инфраструктуры, в том числе не обеспечивающая осуществление критически важных процессов, будет признаваться предметом ст. 274.1 УК РФ. При таком подходе теряется социально-правовой смысл данной нормы, ее дифференцирующее значение.

Довольно сложным вопросом является определение индивидуализирующих признаков вредоносной компьютерной программы и компьютерной информации, указанных в ч. 1 ст. 274.1 УК РФ. В диспозиции указано, 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 «вредонос» 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. 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 компьютерных 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. Подчеркивается, 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).

Неопределенность предмета преступления, предусмотренного 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 Министерства здравоохранения РФ. 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 была оправдана по предъявленному обвинению в соверше-

нии преступления, предусмотренного ч. 1 ст. 274.1 УК РФ[1].

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 фиктивной вакцинации, содеянное необходимо квалифицировать как неправомерный доступ к компьютерной информации (ч. 2 ст. 274.1 УК РФ)[2].

Можно сказать, что «ахиллесовой пятой» уголовно-правовой нормы об ответственности за неправомерное воздействие на объекты критической информационной инфраструктуры Российской Федерации 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. 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 причиняемого вреда [15, с. 103]. 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 данного признака не было разъяснено и в Постановлении Пленума Верховного Суда РФ № 37 от 15 декабря 2022 г.

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. Чекунов в разрешении данного вопроса предлагают опираться на понятие компьютерного инцидента, сформулированного п. 5 ст. 2 Федерального закона от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Этот подход является наиболее расширительным и позволяет относить к категории вреда по смыслу ст. 274.1 УК РФ: 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 [16, с. 32].

Другого мнения придерживается Р. Р. Гайфутдинов, обосновывая, что нельзя отождествлять воздействие на информацию, содержащуюся в критической инфраструктуре, и само причинение вреда инфраструктуре. В случаях, когда противоправное деяние затрагивает исключительно данные, автор предлагает ква-

[1] Приговор Брянского районного суда Брянской области от 28.04.2022 г. по делу № 1-14/2022 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/65072117 (дата обращения: 29.01.2023).

[2] Приговор Армянского городского суда Республики Крым от 19.10.2022 г. по делу № 1-89/2022 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/7163600/ (дата обращения: 29.01.2023).

лифицировать содеянное по ст. 272 УК РФ [17, с. 106].

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[1]; 2) нарушение состояния защищенности и конфиденциальности сведений, содержащихся в критической информационной инфраструктуре[2]; 3) изменение конфигурации элементов информационной системы субъекта критической информационной инфраструктуры, нарушение процесса предоставления услуг связи абонентам[3] и др.

Полагаем, что окончательное решение обозначенной проблемы применения ст. 274.1 УК РФ возможно только путем внесения соответствующих дополнений в Постановление Пленума Верховного Суда РФ № 37 от 15 декабря 2022 г.

Особо следует отметить, что суды обоснованно исключают репутационный вред из возможных негативных последствий деяний, предусмотренных ч. 2 и 3 ст. 274.1 УК РФ. Как совершенно справедливо отмечается в подобных решениях, репутационный вред не может быть причинен объекту критической информационной инфраструктуры, а только ее правообладателю[4].

В правоприменительной практике можно обнаружить примеры неполной квалификации при осуществлении неправомерного воздействия на объекты критической информационной инфраструктуры. Так, например, при совершении распределенных атак на категорированные сетевые ресурсы с последующим отказом системы и блокированием доступа к информации содеянное квалифицируется исключительно как использование вредоносной компьютерной информации по ч. 1 ст. 274.1 УК РФ[5]. Соответственно, необоснованно оставлено без внимания то обстоятельство, что компьютерная атака завершилась причинением вреда критической информационной инфраструктуре, а само использование вредоносной программы явилось способом осуществления неправомерного доступа, т. е. деяния, предусмотренного ч. 2 ст. 274.1 УК РФ. Полагаем, что правильно подобные действия 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 при-

[1] Приговор Бежицкого районного суда города Брянска от 05.08.2022 г. по делу № 1-240/2022 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/ (дата обращения: 29.01.2023).

[2] Приговор Октябрьского районного суда города Владимира от 21.11.2022 г. по делу № 1-351/2022 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/ (дата обращения: 29.01.2023).

[3] Приговор Ленинского районного суда г. Владивостока от 07.10.2020 по делу № 1-366/2020 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/ (дата обращения: 29.01.2023).

[4] Апелляционное определение Ивановского областного суда от 23.12.2022 г. по делу № 22-2476/2022 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/ (дата обращения: 29.01.2023).

[5] Приговор Харабалинского районного суда Астраханской области от 21.12.2022 г. № 1-237/2022 // Судебные решения РФ: сайт. URL: https://судебныерешения.рф/ (дата обращения: 29.01.2023).

знать, что положения отечественного уголовного законодательства об 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 [18]. Вместе с тем до настоящего времени законодателем шаги 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.

В отечественной науке уголовного права исследование проблем противодействия неправомерному воздействию на критическую информационную инфраструктуру Российской Федерации продолжается [19; 20]. Можно с уверенностью говорить о том, что имеющаяся теоретическая дискуссия с опорой на тенденции правоприменения приведет к значимым решениям как на уровне совершенствования законодательства, так и в аспекте деятельности Пленума Верховного Суда РФ.

Выводы

В завершение проведенного исследования целесообразно, насколько это возможно, оценить в целом состояние правоприменительной практики по делам о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации.

Прежде всего надо отметить все возрастающую востребованность исследуемой нормы – наблюдается постоянный рост зарегистрированных преступлений по ст. 274.1 УК РФ.

Очевидным трендом реализации ст. 274.1 УК РФ является ее использование применительно к случаям нарушения правил эксплуатации средств хранения компьютерной информации работниками компаний, оказывающих услуги в сфере связи.

Предсказуемо на уровне судебно-следственной практики наблюдается расхождение в толковании общественно опасных последствий в виде вреда объекту критической информационной инфраструктуры Российской Федерации. Единый доктринальный подход в этом вопросе к настоящему моменту отсутствует.

Следует признать ошибочным встречающееся на практике решение о квалификации содеянного по ч. 1 ст. 274.1 УК РФ в ситуациях, связанных с внесением заведомо недостоверных сведений в категорированные базы данных субъекта критической информационной инфраструктуры. В этом отношении заслуживают поддержки выносимые судами оправдательные приговоры по данному обвинению. Указанные действия, связанные с модификацией информации, образуют признаки преступления, предусмотренного ч. 3 ст. 274.1 УК РФ.

Компьютерные атаки на системы, обеспечивающие критически важные функции, на практике довольно часто сопряжены с требованием передачи денежных средств за прекращение совершаемых действий. Положения отечественного уголовного законодательства об ответственности за вымогательство в этом случае не применимы, поскольку содержанием угрозы является блокирование либо уничтожение компьютерной информации. Решением проблемы могло бы стать дополнение диспозиции ст. 163 УК РФ соответствующей оговоркой об угрозе неправомерного уничтожения, модификации либо блокирования компьютерной информации.

Список литературы

1. Барков А. В., Киселев А. С. Влияние цифровизации на правовое обеспечение информационной безопасности государства и бизнеса в условиях современных геополитических вызовов // Безопасность бизнеса. 2022. № 3. С. 3–7.

2. Барков А. В., Киселев А. С. О правовом обеспечении безопасности информационно-телекоммуникационной инфраструктуры банков и государственных структур // Банковское право. 2022. № 4. С. 20–27.

3. Жарова А. К. Правовое регулирование отношений в области предотвращения возможных уязвимостей в информационных технологиях // Безопасность бизнеса. 2022. № 1. С. 19–26.

4. Противодействие преступлениям, совершаемым в сфере информационных технологий / А. В. Андреев, В. В. Гончар, Н. Н. Горач [и др.]. М.: ИНФРА-М, 2023. 642 с.

5. Риски цифровизации: виды, характеристика, уголовно-правовая оценка: монография / отв. ред. Ю. В. Грачева. М.: Проспект, 2022. 272 с.

6. Русскевич Е. А. Уголовное право и «цифровая преступность»: проблемы и решения: монография. М.: ИНФРА-М, 2019. 227 с.

7. Горян Э. В. Институциональные механизмы обеспечения безопасности критической информационной инфраструктуры Российской Федерации и Сингапура: сравнительно-правовой аспект // Административное и муниципальное право. 2018. № 9. С. 49–60.

8. 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.

9. Пыхтин И. Г. Уголовно-правовая охрана объектов критической информационной инфраструктуры как одно из ключевых направлений современной борьбы с киберпреступностью в Российской Федерации // Известия Юго-Западного государственного университета. Серия: История и право. 2018. Т. 8, № 1 (26). С. 98–103.

10. 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. 108–113.

11. Пыхтин И. Г. Обеспечение уголовно-правовой охраны национальных объектов критической информационной инфраструктуры Германии, Австрии, Швейцарии и Франции // Известия Юго-Западного государственного университета. Серия: История и право. 2019. Т. 9, № 2 (31). С. 108–115.

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

13. Ефремова М. А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. № 4 (50). С. 86–92.

14. 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.

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

16. Русскевич Е. А., Чекунов И. Г. Квалификация неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации // Уголовное право. 2022. № 5. С. 26–35.

17. Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации: дис. … канд. юрид. наук. Казань, 2017. 243 с.

18. Тирранен В. А. Проблема уголовной ответственности за криптовирусные атаки // Уголовное право: стратегия развития в XXI в.: материалы XV Международной научно-практической конференции (Москва, 25-26 января 2018 г.). М.: РГ-Пресс, 2018. С. 637–640.

19. Пыхтин И. Г. Логико-языковые феномены предмета неправомерного воздействия на критическую информационную инфраструктуру России (ст. 274.1 УК РФ) // Вестник Российской правовой академии. 2021. № 1. С. 118–124.

20. Новичков В. Е., Пыхтин И. Г. Конфликт научно-отраслевых интересов при определении понятия информационной безопасности Российской Федерации: уголовно-правовой подход // Известия Юго-Западного государственного университета. Серия: История и право. 2018. Т. 8, № 4 (29). С. 167–178.

References

1. Barkov A. V., Kiselev A. S. Vliyanie cifrovizacii na pravovoe obespechenie informacionnoj bezopasnosti gosudarstva i biznesa v usloviyah sovremennyh geopoliticheskih vyzovov [The impact of digitalization on the legal support of information security of the state and business in the context of modern geopolitical challenges]. *Bezopasnost' biznesa = Business Security*, 2022, no. 3, pp. 3–7.

2. Barkov A. V., Kiselev A. S. O pravovom obespechenii bezopasnosti informacionno-telekommunikacionnoj infrastruktury bankov i gosudarstvennyh struktur [On the legal security of the information and telecommunication infrastructure of banks and state structures]. *Bankovskoe pravo = Banking law*, 2022, no. 4, pp. 20–27.

3. Zharova A. K. Pravovoe regulirovanie otnoshenij v oblasti predotvrashcheniya vozmozhnyh uyazvimostej v informacionnyh tekhnologiyah [Legal regulation of relations in the field of prevention of possible vulnerabilities in information technologies]. *Bezopasnost' biznesa = Business security*, 2022, no. 1, pp. 19–26.

4. Andreev A. V., Gonchar V. V., Gorach N. N., eds. Protivodejstvie prestupleniyam, sovershaemym v sfere informacionnyh tekhnologij [Counteraction to crimes committed in the field of information technology]. Moscow, INFRA-M Publ., 2023, 642 p.

5. Riski cifrovizacii: vidy, harakteristika, ugolovno-pravovaya ocenka [Risks of digitalization: types, characteristics, criminal law assessment]; ed. by Yu.V. Grachev. Moscow, Prospekt Publ., 2022, 272 p.

6. Russkevich E. A. Ugolovnoe pravo i "cifrovaya prestupnost'": problemy i resheniya [Criminal law and "digital crime": problems and solutions]. Moscow, INFRA-M Publ., 2019. 227 p.

7. Goryan E. V. Institucional'nye mekhanizmy obespecheniya bezopasnosti kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii i Singapura: sravnitel'no-pravovoj aspekt [Institutional mechanisms for ensuring the security of the critical information infrastructure of the Russian Federation and Singapore: a comparative legal aspect]. *Administrativnoe i municipal'noe pravo = Administrative and municipal law*, 2018, no. 9, pp. 49–60.

8. Reshetnikov A. Yu., Russkevich E. A. Ob ugolovnoj otvetstvennosti za nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii (st. 274.1 UK Rossii) [On criminal liability for unlawful impact on the critical information infrastructure of the

Russian Federation (Article 274.1 of the Criminal Code of Russia)]. *Zakony Rossii: opyt: analiz, praktika = Laws of Russia: experience: analysis, practice,* 2018, no. 2 (66), pp. 51–55.

9. Pykhtin I. G. Ugolovno-pravovaya ohrana ob"ektov kriticheskoj informacionnoj infrastruktury kak odno iz klyuchevyh napravlenij sovremennoj bor'by s kiberprestupnost'yu v Rossijskoj Federacii [Criminal Law Protection of Critical Information Infrastructure Objects as One of the Key Directions of the Modern Fight against Cybercrime in the Russian Federation]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law,* 2018, vol. 8, no. 1 (26), pp. 98–103.

10. Russkevich E. A. Ugolovnaya otvetstvennost' za prestupleniya v sfere komp'yuternoj informacii po zakonodatel'stvu Kitajskoj Narodnoj Respubliki: sravnitel'no-pravovoj analiz [Criminal liability for crimes in the field of computer information under the legislation of the People's Republic of China: a comparative legal analysis]. *Zhurnal zarubezhnogo zakonodatel'stva i sravnitel'nogo pravovedeniya = Journal of Foreign Legislation and Comparative Law,* 2018, no. 5, pp. 108–113.

11. Pykhtin I. G. Obespechenie ugolovno-pravovoj ohrany nacional'nyh ob"ektov kriticheskoj informacionnoj infrastruktury Germanii, Avstrii, Shvejcarii i Francii [Ensuring criminal law protection of national objects of critical information infrastructure in Germany, Austria, Switzerland and France]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law,* 2019, vol. 9, no. 2 (31), pp. 108–115.

12. Begishev I. R. Bezopasnost' kriticheskoj informacionnoj infrastruktury Rossijskoj Federacii [Security of the critical information infrastructure of the Russian Federation]. *Bezopasnost' biznesa = Business security,* 2019, no. 1, pp. 27–32.

13. Efremova M. A. Ugolovnaya otvetstvennost' za nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii [Criminal liability for unlawful impact on the critical information infrastructure of the Russian Federation]. *Vestnik Kazanskogo yuridicheskogo instituta MVD Rossii = Bulletin of the Kazan Law Institute of the Ministry of Internal Affairs of Russia,* 2022, no. 4 (50), pp. 86–92.

14. Kruglikov L. L., Brazhnik S. D., Pilyasov I. A. Nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii (st. 274.1 UK RF): nekotorye problemy opredeleniya priznakov sostava prestupleniya [Unlawful impact on the critical information infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation): some problems in determining the signs of a crime]. *Zhurnal yuridicheskih issledovanij = Journal of Legal Studies,* 2019, vol. 4, no. 3, pp. 53–62.

15. Truntsevsky Yu. V. Nepravomernoe vozdejstvie na kriticheskuyu informacionnuyu infrastrukturu: ugolovnaya otvetstvennost' ee vladel'cev i ekspluatantov [Unlawful impact on critical information infrastructure: criminal liability of its owners and operators]. *Zhurnal rossijskogo prava = Journal of Russian Law,* 2019, no. 5, pp. 99–106.

16. Russkevich E. A., Chekunov I. G. Kvalifikaciya nepravomernogo vozdejstviya na kriticheskuyu informacionnuyu infrastrukturu Rossijskoj Federacii [Qualification of illegal impact on the critical information infrastructure of the Russian Federation]. *Ugolovnoe pravo = Criminal law,* 2022, no. 5, pp. 26–35.

17. Gayfutdinov R. R. Ponyatie i kvalifikaciya prestuplenij protiv bezopasnosti komp'yuternoj informacii. Diss. kand. yurid. nauk [The concept and qualification of crimes against the security of computer information. Cand. legal sci. diss.]. Kazan, 2017. 243 p.

18. Tirranen V. A. [The problem of criminal liability for cryptovirus attacks]. *Ugolovnoe pravo: strategiya razvitiya v XXI v. Materialy XV Mezhdunarodnoj nauchno-prakticheskoj kon-*

ferencii [Criminal law: development strategy in the XXI century. Materials of the XV International Scientific and Practical Conference]. Moscow, RG-Press Publ., 2018, pp. 637–640.

19. Pykhtin I. G. Logiko-yazykovye fenomeny predmeta nepravomernogo vozdejstviya na kriticheskuyu informacionnuyu infrastruktury Rossii (st. 274.1 UK RF) [Logical and linguistic phenomena of the subject of unlawful influence on the critical information infrastructure of Russia (Article 274.1 of the Criminal Code of the Russian Federation)]. *Vestnik Rossijskoj pravovoj akademii = Bulletin of the Russian Legal Academy,* 2021, no. 1, pp. 118–124.

20. Novichkov V. E., Pykhtin I. G. Konflikt nauchno-otraslevyh interesov pri opredelenii ponyatiya informacionnoj bezopasnosti Rossijskoj Federacii: ugolovno-pravovoj podhod [Conflict of scientific and branch interests in defining the concept of information security of the Russian Federation: a criminal law approach]. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Istoriya i pravo = Proceedings of the Southwest State University. Series: History and Law,* 2018, vol. 8, no. 4 (29), pp. 167–178.

Информация об авторе / Information about the Author

Малыгин Иван Игоревич, консультант, отдел государственной регистрации нормативных правовых актов в социальной и культурной сферах, Департамент регистрации ведомственных нормативных правовых актов, Министерство юстиции Российской Федерации,
г. Москва, Российская Федерация,
e-mail: aspugpravo@yandex.ru
ORCID: 0009-0008-0830-5614

Ivan I. Malygin, Consultant, Department of State Registration of Normative Legal Acts in the Social and Cultural Spheres, Department of Registration of Departmental Legal Acts, Ministry of Justice of the Russian Federation,
Moscow, Russian Federation,
e-mail: aspugpravo@yandex.ru
ORCID: 0009-0008-0830-5614