ISSN 2500-1442

Научная статья
УДК 343.34
EDN OLQBCA
DOI 10.17150/2500-1442.2023.17(1).22-34

ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

И.Н. Мосечкин
Вятский государственный университет, г. Киров, Российская Федерация

Информация о статье

Дата поступления
3 ноября 2022 г.

Дата принятия в печать
21 февраля 2023 г.

Дата онлайн-размещения
13 марта 2023 г.

Ключевые слова

Компьютерная информация; вирус; вредоносная программа; неправомерный доступ; критическая информационная инфраструктура; компьютерная атака; компьютерный инцидент

Аннотация. Статья посвящена проблемам совершенствования уголовно-правовых норм, регулирующих ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Актуальность темы исследования обусловлена ростом количества данных преступлений и новизной ст. 274.1 УК РФ. Статистические сведения свидетельствуют о крайне высоком числе компьютерных атак на критическую информационную инфраструктуру, однако преступлений регистрируется значительно меньше. В качестве одной из причин сложившейся ситуации может выступать несовершенство ст. 274.1 УК РФ. Автор обращает внимание на то, что ч. 1 ст. 274.1 УК РФ не отвечает основаниям криминализации, а ее юридическая конструкция препятствует эффективной работе сотрудников следственных и судебных органов. Это приводит к тому, что распространенное общественно опасное деяние не находит должного отражения в судебно-следственной практике. В то же время действующая ст. 273 УК РФ обладает достойным потенциалом для охвата неправомерных создания, распространения и (или) использования каких-либо компьютерных программ в отношении критической информационной инфраструктуры или информации, содержащейся в ней. Автор отмечает, что применяемое в действующей редакции ст. 274.1 УК РФ понятие «вред критической информационной инфраструктуре Российской Федерации» является неконкретизированным, порождающим промедление, ошибки и недоразумения в юридической практике. В статье доказывается, что ч. 2 и 3 ст. 274.1 УК РФ могли бы обеспечить лучшее взаимодействие с иными нормативными актами, если бы их диспозиции включали категории «компьютерная атака» и «компьютерный инцидент». Введение указанных признаков могло бы поспособствовать единообразию в судебной практике и устранению неоднозначных толкований. Изучение субъективной стороны преступлений, предусмотренных ст. 274.1 УК РФ, позволило сделать вывод о целесообразности учета в качестве квалифицирующих признаков корыстного мотива и цели скрыть другое преступление или облегчить его совершение. В качестве обоснования данной позиции в работе указывается на распространенность этих признаков, использование их при конструировании иных составов, а также мнение ученых-правоведов.

Original article

PROBLEMS OF THE CRIMINAL LAW PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Ilya N. Mosechkin
Vyatka State University, Kirov, the Russian Federation

Article info

Received
2022 November 3

Accepted
2023 February 21

Available online
2023 March 13

Abstract. The article discusses the problems of improving criminal law norms regulating liability for unlawful impact on critical information infrastructure of the Russian Federation. The urgency of the research topic is connected with a growing number of such crimes and the recent adoption of Art. 274.1 of the Criminal Code of the Russian Federation. According to statistics, the number of attacks against critical information infrastructure is extremely high, however, a considerably smaller number of incidents are registered as crimes. One of the reasons behind this situation is the inadequacy of Art. 274.1 of the CC of the RF. The author draws attention to the fact that Part 1 of Art. 274.1 of the CC of the RF does not meet the criteria for criminalization, and

Keywords

Computer information; virus; malware; unauthorized access; critical information infrastructure; computer attack; computer incident

its legal construction hinders the effective work of investigation and court bodies' employees. As a result, this widespread publicly dangerous act is not duly reflected in judicial and investigation practice. At the same time, the current Art. 273 of the CC of the RF has considerable potential for including unlawful creation, dissemination and (or) use of any computer software in relation to critical information infrastructure or information contained in it. The author notes that the concept used in the current edition of Art. 274.1 of the CC of the RF «harm to the critical information infrastructure of the Russian Federation» is non-specific, and leads to delays, mistakes and confusion in legal practice. The article proves that Parts 2 and 3 of Art. 274.1 of the CC of the RF could ensure better liaison with other legal acts if their dispositions included the categories «computer attack» and «computer incident». The introduction of the above-mentioned attributes could also contribute to the consistency of court practice and the elimination of ambiguous interpretations. The analysis of the subjective side of crimes under Art. 274.1 of the CC of the RF allowed the author to conclude that mercenary motivation and the goal of concealing or aiding another crime should be viewed as qualifying features. To prove this position, the author points out that these features are wide-spread and used for the construction of corpus delicti of other crimes, and also cites the opinions of legal scholars.

Введение

Развитие науки и техники продолжается стремительными темпами. Можно с уверенностью сказать, что до предельной границы цифровизации еще весьма далеко, поэтому внедрение новых и совершенствование уже внедренных технологий будет неразрывно связано с деятельностью человека на протяжении длительного времени. К сожалению, почти все, что было создано для улучшения жизни людей, может быть использовано также в противоправных целях. Киберпреступность является ярким тому примером.

Последние несколько лет наблюдается тенденция к увеличению числа преступлений, совершаемых с помощью компьютерных технологий. Ограничения, которые вводились во время пандемии, оказали существенное влияние на количество цифровых правонарушений, поскольку и законопослушные лица, и нарушители стали проводить больше времени в интернет-пространстве. Однако, как показывают современные исследования, освобождение от карантинных ограничений не привело к замедлению роста числа противоправных деяний. Это объясняется в том числе и тем, что повседневная рутинная деятельность теперь во многом осуществляется в цифровой среде: медицинские консультации, образовательные услуги, покупки и развлечения [1].

Проблема противодействия компьютерным преступлениям обостряется вследствие не только их количественных, но и качественных изменений: появляются новые способы противоправных посягательств, орудия и средства, а также риски в различных сферах общественных отношений, связанных, например, с применением искусственного интеллекта [2, с. 5] или эксплуатацией робототехники [3, с. 142]. Законодатель реагирует на эволюцию преступлений в сфере компьютерной информации, хотя не всегда своевременно. На момент вступления в законную силу Уголовный кодекс Российской Федерации предусматривал ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных программ для ЭВМ, а также нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети. В дальнейшем ст. 272–274 УК РФ неоднократно подвергались изменениям, продиктованным преобразованиями в развитии и распространении компьютерной техники. К примеру, в уголовном законе произошел переход от категории «ЭВМ» к категории компьютерной информации в целом.

Сейчас трудно представить эффективное управление сложными процессами без использования данной информации. В то же время зарубежные ученые верно утверждают, что недостатки в системе безопасности позволяют злоумышленникам создавать обширные наборы зараженных объектов, что в дальнейшем может быть использовано для эксплуатации других объектов, манипулирования организациями и, возможно, разрушения стран и экономики. Такой вывод обоснован эволюционными тенденциями последнего десятилетия [4, p. 242]. Всеобщая цифровизация также послужила почвой для возникновения такого негативного противоправного явления, как кибертерроризм. Его приверженцы выбирают сферы, нападение на которые может привести к наиболее разрушительным последствиям: энергетика, здравоохранение, финансы, деятельность экстренных служб [5, с. 383].

Осознание принципиальных различий в характере и степени общественной опасности посягательств на компьютерную информацию отдельного человека и посягательств на системы, обеспечивающие деятельность множества лиц, привело к соответствующим изменениям в законодательстве. В ряде стран совокупность особо значимых объектов стали относить к критической информационной инфраструктуре с присущими ей особенностями правового регулирования. Например, в Южной Корее с 2001 г. действует Закон о защите информационно-коммуникационной инфраструктуры (Act on the protection of information and communications infrastructure), которым распределены обязанности по защите наиболее важной информации и информационной инфраструктуры. Кроме того, данным нормативным актом установлены принципы такой защиты, запрет определенных действий и достаточно суровые санкции в случае совершения посягательств [6, p. 880]. В Европейском союзе с 2008 г. действует директива 2008/114/ЕС, в которой дается понятие критической инфраструктуры, охватывающее информационные и коммуникационные технологии. При этом государствам-членам предписывается предпринимать ряд усилий для недопущения прекращения функционирования наиболее важных элементов этой инфраструктуры. Отдельно обращается внимание на транснациональный характер и взаимосвязь критической информационной инфраструктуры различных государств [7]. В Китайской Народной Республике в 2016 г. в законодательство были внесены изменения, направленные на усиление мер по обеспечению кибербезопасности. Предусмотрено понятие критической информационной инфраструктуры и регламентированы условия обеспечения ее специальной защиты [8, p. 1342].

В Российской Федерации до 2017 г. регулирование данной сферы осуществлялось несколькими отдельными нормативными актами. Однако отсутствие полноценного системного подхода, наличие недостатков и пробелов в законодательстве, а также зарубежный опыт обусловили необходимость формирования иного подхода. Поэтому был разработан, а в 2017 г. принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ, который, без преувеличения, стал одним из важнейших инструментов обеспечения информационной безопасности[1]. Ученые отмечают, что указанный нормативный акт способствует предотвращению угроз кибербезопасности, которые исходят от высококвалифицированных, осведомленных в области информационных технологий преступных киберсообществ, охватывающих в своей деятельности даже государственные уровни [9].

Однако всесторонняя защита важнейших общественных отношений невозможна без уголовного права. Для противодействия посягательствам на отдельные информационные системы и автоматизированные системы управления, а также для дифференциации ответственности за них в УК РФ была введена ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Преступления, предусмотренные вышеуказанной статьей, не являются распространенными по сравнению с традиционными деликтами, однако отмечается рост их количества. Согласно данным ГИАЦ МВД России, за 2018–2021 гг. число противоправных актов составило 186: в 2018 г. было зарегистрировано 1 преступление, в 2019 г. — 4, в 2020 г. — 22, а в 2021 г. — 159[2]. Таким образом, ст. 274.1 УК РФ нашла отражение в судебно-следственной практике. В то же время организации, обеспечивающие кибербезопасность, отчитываются о гораздо большем количестве компьютерных атак на критическую информационную инфраструктуру Российской Федерации (КИИ РФ). В частности, согласно данным Национального координационного центра по компьютерным инцидентам, только в 2018 г. в отношении России было совершено более 4,3 млрд кибератак на КИИ РФ. И это число с каждым годом увеличивается [10]. Существует множество причин расхождения между количеством зарегистрированных преступлений и количеством компьютерных атак, однако не последней из них является несовершенство закона.

Введение ст. 274.1 УК РФ привело к появлению в научной среде критических замечаний, часть из которых хорошо аргументирована, обоснована и заслуживает внимания [11, с. 200; 12,

[1] О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26 июля 2017 г. № 187-ФЗ // Российская газета. 2017. 31 июля.

[2] Данные предоставлены ФКУ «ГИАЦ МВД РФ» по запросу автора.

с. 183]. С другой стороны, проблемам уголовно-правовой защиты КИИ РФ посвящено достаточно малое количество трудов, что говорит о необходимости дальнейших научных исследований данной тематики.

Основное исследование

Статья 274.1 УК РФ содержит признаки сразу трех самостоятельных составов преступления. В частности, в ч. 1 предусмотрена ответственность за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на КИИ РФ. Часть 2 ст. 274.1 УК РФ запрещает неправомерный доступ к охраняемой компьютерной информации, содержащейся в КИИ РФ. В ч. 3 предусмотрена ответственность за нарушение различных правил эксплуатации и правил доступа, связанных с функционированием КИИ РФ.

Несмотря на значительные различия между указанными составами, законодатель в последних двух частях ст. 274.1 УК РФ закрепил квалифицирующие признаки сразу по отношению ко всем, без учета каких-либо особенностей. Так, увеличение степени общественной опасности деяния связывается с наличием различных форм соучастия, использованием виновным лицом своего служебного положения или наступлением тяжких последствий. Диспозиции норм сформулированы по типу бланкетных, поэтому для их применения и толкования необходимо учитывать положения, закрепленные в других источниках. К их числу можно отнести федеральный закон от 26 июля 2017 г. № 187-ФЗ, федеральный закон от 27 июля 2006 г. № 149-ФЗ и ряд иных[3]. Закрепленные в данных актах положения имеют огромное значение для межотраслевого регулирования сферы информационно-телекоммуникационных технологий.

Исходя из размещения ст. 274.1 в гл. 28 УК РФ, а также учитывая положения Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ, в качестве объекта преступлений, предусмотренных в ст. 274.1 УК РФ, можно определить общественные отношения, обеспечивающие безопасность КИИ РФ и информации, содержащейся в ней. На наш взгляд, указанные преступления также являются многообъектными. Во-первых, информационные системы и автоматизированные системы управления обеспечивают нормальную деятельность в самых разных сферах: транспортной, медицинской, энергетической, банковской и иных. Соответственно, посягательства на КИИ РФ причиняют вред и этим сферам. Во-вторых, ч. 5 ст. 274.1 УК РФ содержит признак наступления тяжких последствий, которые могут проявляться в виде крупных аварий, остановок производственных процессов или имущественного вреда. Иначе говоря, факультативными объектами являются общественные отношения, обеспечивающие безопасность собственности, экономической деятельности, конституционного строя, правосудия и др.

Пункты 6 и 7 федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» дают основания говорить о том, что предметом преступлений, предусмотренных ст. 274.1 УК РФ, являются: КИИ РФ, сети электросвязи, используемые для организации взаимодействия объектов КИИ РФ, информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ РФ.

Объективная сторона состава преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, выражается в трех альтернативных действиях:

– создание компьютерных программ либо компьютерной информации;

– распространение таких программ или информации;

– их использование.

Обязательным признаком компьютерных программ либо компьютерной информации является их предназначение для неправомерного воздействия на КИИ РФ (охватывающего, помимо прочего, уничтожение, блокирование, модификацию, копирование информации или нейтрализацию средств защиты). Деяния совершаются в форме активных действий. По конструкции объективной стороны состав формальный.

Представляется достаточно очевидным, что при конструировании состава преступления, предусмотренного ч. 1 ст. 274.1 УК РФ, законодатель принимал во внимание положения, закрепленные в ст. 273 УК РФ. По крайней мере, перечень альтернативных действий совпадает. Важное отличие заключается в предназначении создаваемых, распространяемых или используемых программ: согласно ч. 1 ст. 274.1 УК РФ,

[3] Об информации, информационных технологиях и о защите информации : федер. закон от 27 июля 2006 г. № 187-ФЗ : (ред. от 14 июля 2022 г.) // Российская газета. 2006. 29 июля.

они должны быть ориентированы именно на неправомерное воздействие на КИИ РФ, а не любую компьютерную информацию. При этом такое воздействие влечет за собой не только уничтожение, блокирование, модификацию, копирование информации или нейтрализацию средств ее защиты, но и другие возможные результаты, на что указывает юридическая конструкция «в том числе».

Среди требований к криминализации того или иного деяния в научной литературе выделяют его общественную опасность, распространенность, а также непригодность иных правовых запретов для устранения возникшей опасности [13]. На наш взгляд, ч. 1 ст. 274.1 УК РФ не вполне отвечает названным требованиям. Да, общественная опасность создания, использования и распространения вредоносных программ неоспорима. Однако она уже учтена законодателем в ст. 273 УК РФ, которая пусть и нуждается в совершенствовании, но применяется весьма активно. Думается, что одно лишь предназначение программы для воздействия на КИИ РФ не столь существенно повышает степень общественной опасности деяния, чтобы вводить специальный состав преступления. В противном случае можно было бы закрепить отдельные статьи, предусматривающие ответственность за создание программ, направленных на посягательства на жизнь, честь и достоинство, конституционные права и свободы и иные. К тому же санкция, закрепленная в ч. 1 ст. 274.1 УК РФ, незначительно отличается от санкций, закрепленных в ст. 273 УК РФ.

По мнению Л.И. Федосеева, практически невозможно определить предназначение программы для воздействия исключительно в отношении объектов КИИ РФ, так как в таком случае и средства обеспечения защиты должны быть уникальными, что маловероятно [14, с. 191]. Ряд ученых дополняют этот вывод тем, что широкое толкование «предназначенности» охватит любые вредоносные программы, а узкое — не позволит охватить средство, специально разработанное под отдельный объект КИИ [15, с. 136]. Статистические сведения показывают: при отсутствии разъяснений Пленума Верховного Суда Российской Федерации чаще всего используется узкое толкование. Не в последнюю очередь из-за этого за четыре года действия ч. 1 ст. 274.1 УК РФ (2018–2021) количество осужденных составило всего 5 чел.[4]

Между тем в практике встречается не совсем корректное, на наш взгляд, применение нормы к случаям неправомерного использования программ, не предназначенных исключительно для воздействия на КИИ РФ. В частности, как следует из постановления Кировского районного суда г. Махачкалы о прекращении уголовного дела 1-442/2022, Г. И. Р. заинтересовался тематикой DDoS-атак (распределенные сетевые атаки типа «отказ в обслуживании») и стал ее изучать на различных ресурсах в сети Интернет. В конце апреля 2021 г. Г. И. Р., собрав достаточные познания в области совершения DDoS-атак, решил блокировать работу веб-серверов организаций, деятельность которых обеспечивала электросвязь. Федеральной службой по техническому и экспортному контролю России организации отнесены к субъектам КИИ РФ, а их информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления — к объектам КИИ РФ. Г. И. Р. из любопытства осуществил вход на сайты, предназначенные для блокирования компьютерной информации, и путем ввода доменных имен и IP-адреса задал команды о совершении атак по уровню Layer 4, нацеленных на достижение пределов по ширине канала по количеству допустимых подключений и нарушение работы сетевого оборудования. Он же задал команды о совершении атак по уровню Layer 7, нацеленных на чрезмерное потребление системных ресурсов службами на атакуемом сервере. Совершенные Г. И. Р. компьютерные атаки привели к блокированию компьютерной информации, невозможности осуществлять требуемые операции и затруднению доступа законных пользователей. Уголовное дело было прекращено в связи с примирением с потерпевшим[5].

Как следует из указанного постановления, виновное лицо применяло программы, предназначенные для осуществления DDoS-атак, использующие ограничения пропускной способности, характерные для любых сетевых ресурсов. Специалистам в области кибербезопасности такие виды программ широко известны — они были созданы достаточно давно, еще до появления федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации». Следовательно, едва

[4] Данные о назначенном наказании по статьям УК // Судебная статистика РФ. URL: https://stat.xn----7sbqk8achja.xn--p1ai.

[5] Постановление Кировского районного суда г. Махачкалы Республики Дагестан от 21 июня 2022 г. по делу 1-442/2022 о прекращении уголовного дела // ГАС «Правосудие».

ли такую программу можно назвать предназначенной именно для воздействия на КИИ РФ.

В целом весьма распространенное общественно опасное деяние не находит должного отражения в судебно-следственной практике из-за неудачной юридической конструкции и не совсем оправданного выделения специального состава. В свою очередь, нельзя говорить и о непригодности иных правовых запретов для устранения возникшей опасности, поскольку ст. 273 УК РФ применяется часто, а практические работники хорошо знакомы с особенностями толкования и применения нормы.

Изложенное позволяет сделать вывод о том, что острой необходимости в ч. 1 ст. 274.1 УК РФ не имеется, по крайней мере в действующей редакции. Возможно, законодателю следовало бы включить в объективную сторону общественно опасные действия, которые еще не предусмотрены в других статьях уголовного закона. Однако, как нам представляется, наличие ч. 1 ст. 274.1 УК РФ в целом неоправданно, а существующая юридическая конструкция усложняет деятельность работников судебных и следственных органов. Затруднительно говорить и о соблюдении требований к криминализации. Более того, как следует из ч. 2 ст. 274.1 УК РФ, неправомерный доступ к информации, содержащейся в КИИ РФ, может совершаться с использованием как специально предназначенных для этого программ, так и иных вредоносных компьютерных программ. То есть в этом случае законодатель не увидел необходимости дифференциации ответственности.

На наш взгляд, целесообразно вообще исключить ч. 1 ст. 274.1 из УК РФ в текущем или каком бы то ни было виде. При этом речь не идет о полной декриминализации предусмотренных в ней деяний, так как ст. 273 УК РФ обладает необходимым потенциалом для противодействия созданию, использованию или распространению вредоносных программ. Более того, квалифицирующие признаки в ней отражены даже лучше, поскольку охватывают крупный ущерб, корыстную заинтересованность и угрозу наступления тяжких последствий. Однако оправданно также будет скорректировать пределы закрепленных в статье санкций с учетом возможного посягательства на КИИ РФ. Таким образом, в рамках предлагаемых нами изменений создание, распространение, а также использование вредоносных компьютерных программ (в том числе предназначенных для неправомерного воздействия на КИИ РФ) следует квалифицировать по ст. 273 УК РФ. В том случае если неправомерный доступ к КИИ РФ был получен и это повлекло причинение вреда, содеянное будет образовывать совокупность преступлений, предусмотренных ч. 2 ст. 274.1 и ст. 273 УК РФ.

Объективная сторона состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, включает общественно опасное действие в виде неправомерного доступа к охраняемой компьютерной информации, содержащейся в КИИ РФ, как с использованием специальных (в том числе вредоносных) компьютерных программ, так и без них. Обязательным признаком выступает общественно опасное последствие — вред КИИ РФ. Благодаря системному толкованию данной нормы Е.А. Русскевичу удалось сделать вывод о том, что к такому вреду можно отнести уничтожение, блокирование, модификацию, копирование информации, нейтрализацию средств защиты информации или выведение из строя аппаратных и программных средств, обеспечивающих функционирование КИИ РФ [16, с. 319]. Данная позиция представляется обоснованной и логичной, но неполной, если принимать во внимание сложившуюся практику. Выборочное изучение материалов уголовных дел показывает, что к вреду также относят нарушение безопасности, процессов оказания услуг или иные последствия. В отдельных решениях судов к вреду КИИ РФ относят также дискредитацию деловой репутации, хотя, думается, деловая репутация не является составной частью КИИ РФ[6]. По существу, часто одни и те же последствия в приговорах судов описываются разными словами, что выступает следствием отсутствия конкретизации признака «вред» в ст. 274.1 УК РФ. Между неправомерным доступом и вредом КИИ РФ должна иметь место причинно-следственная связь. Состав является материальным, следовательно, преступление признается оконченным с момента наступления общественно опасных последствий.

Заметно, что при конструировании состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, законодатель принимал во внимание положения, закрепленные в ст. 272 УК РФ. В литературе можно встретить утверждение о том, что диспозиция, содержащаяся в ч. 2 ст. 274.1 УК РФ, по сути, повторяет диспозицию ст. 272 УК РФ, а

[6] Приговор от 29 июля 2020 г. по делу № 1-805/2020 по обвинению К. С. С. в совершении преступления, предусмотренного частью 2 статьи 274.1 УК РФ // ГАС «Правосудие».

единственное различие — указание на иной предмет преступления [17]. Позволим себе не согласиться с данной точкой зрения. Принципиальные различия составов кроются в способах совершения деяния: в одном случае имеет место неправомерный доступ без использования специальных программ, а в другом — доступ охватывает такое использование, а значит, не требует дополнительной квалификации. Кроме того, различными являются также формы общественно опасных последствий: уничтожение, блокирование, модификация и копирование компьютерной информации не совпадают по значению с вредом КИИ РФ. В то же время нельзя отрицать общего сходства составов.

В целом юридическая конструкция ч. 2 ст. 274.1 УК РФ представляется нам весьма спорной. Диспозиция включает признаки составного преступления и охватывает не только неправомерный доступ, но и использование предназначенных, а равно не предназначенных для неправомерного воздействия на КИИ РФ программ. В свою очередь, как верно отмечает Е.А. Русскевич, создание и распространение программ остаются за пределами ч. 2 ст. 274.1 УК РФ, т.е. требуют дополнительной квалификации по ст. 273 или ч. 1 ст. 274.1 УК РФ [16, с. 321]. Подобная конструкция лишь затрудняет работу правоприменителя, что может объяснять низкие показатели зарегистрированных преступлений. Также усугубляет ситуацию неконкретизированный вред КИИ РФ и отсутствие официальных толкований данного общественно опасного последствия.

Вышеуказанных проблем можно было избежать на этапе введения ст. 274.1 в УК РФ, причем все предпосылки для этого имелись. В частности, Федеральный закон «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» от 26 июля 2017 г. № 194-ФЗ и Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ разрабатывались, обсуждались и принимались одновременно как дополняющие друг друга. С одной стороны, появилось общее правовое регулирование КИИ РФ, охватывающее основные вопросы: понятия, принципы, объекты, субъекты и требования к обеспечению безопасности. С другой стороны, обеспечивалась уголовно-правовая защита КИИ РФ, без которой невозможна сохранность столь важных общественных отношений. Взаимосвязь норм несомненна, поэтому вызывает немалое удивление решение законодателя сконструировать ст. 274.1 УК РФ без учета положений федерального закона от 26 июля 2017 г. № 187-ФЗ.

При этом в обширном отечественном опыте законотворчества имеется немало примеров, когда в уголовном законе используются юридические конструкции других нормативных актов. Так, ст. 178 УК РФ запрещает заключение картеля, понятие и признаки которого содержатся в Федеральном законе «О защите конкуренции» от 26 июля 2006 г. № 135-ФЗ. Статья 192 УК РФ предусматривает наказание за уклонение от обязательной сдачи на аффинаж драгоценных металлов, определение которого зафиксировано в Федеральном законе «О драгоценных металлах и драгоценных камнях» от 26 марта 1998 г. № 41-ФЗ. Статья 258 УК РФ не раскрывает признаков охоты, зато их раскрывает Федеральный закон «Об охоте и о сохранении охотничьих ресурсов и о внесении изменений в отдельные законодательные акты Российской Федерации» от 24 июля 2009 г. № 209-ФЗ. Подобные примеры можно приводить еще долго.

Возвращаясь к теме исследования, необходимо обратить внимание на п. 4 ст. 2 федерального закона от 26 июля 2017 г. № 187-ФЗ, в котором содержится понятие «компьютерная атака», охватывающее любое умышленное воздействие на КИИ РФ с применением как вредоносных, так и иных программ и программно-аппаратных средств, если это совершается в целях нарушения или прекращения функционирования объектов КИИ РФ либо создания угрозы безопасности обрабатываемой информации. На наш взгляд, компьютерная атака выступала бы более полным и правильным признаком объективной стороны, нежели неправомерный доступ. В контексте сказанного следует отметить, что доступ к информации означает возможность получения информации и ее использования, если исходить из буквального толкования п. 6 ст. 2 Федерального закона «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ. В свою очередь, компьютерная атака может совершаться и с получением информации, и без получения. Например, при DDoS-атаке генерируется большое количество вредоносных па-

кетов, которые перегружают веб-серверы, что вызывает отказ в обслуживании [18]. При посягательстве с помощью спам-транзакций на технологии блокчейна существенно увеличивается обычная продолжительность транзакций или происходит перегрузка сети [19].

Кроме того, в п. 5 ст. 2 федерального закона от 26 июля 2017 г. № 187-ФЗ раскрывается понятие «компьютерный инцидент». Оно охватывает нарушение и прекращение функционирования объекта КИИ РФ, сети электросвязи, а также нарушение безопасности информации, обрабатываемой объектом КИИ РФ. Компьютерный инцидент, как нам представляется, является более правильным и конкретизированным общественно опасным последствием, чем вред критической информационной инфраструктуре, закрепленный в ч. 2 ст. 274.1 УК РФ. Введение данного признака могло бы поспособствовать единообразию в судебной практике и устранению неоднозначных толкований, по итогам которых к преступным последствиям относят, например, дискредитацию деловой репутации. Таким образом, думается, что юридическая конструкция ч. 2 ст. 274.1 УК РФ должна охватывать общественно опасное деяние в виде компьютерной атаки, а также общественно опасное последствие в виде компьютерного инцидента.

Объективная сторона состава преступления, предусмотренного ч. 3 ст. 274.1 УК РФ, включает общественно опасное деяние в виде нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, а также информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи либо правил доступа к ним. Деяние может быть совершено и в форме действия, и в форме бездействия. Имеется значительное сходство со ст. 274 УК РФ, однако необходимо принимать во внимание бланкетный характер диспозиции. Правила эксплуатации и доступа, связанные с объектами и субъектами КИИ РФ, регулируются иными нормативными актами, предусматривающими гораздо более строгие условия.

Обязательным признаком рассматриваемого состава преступления является общественно опасное последствие — вред КИИ РФ. Ю.В. Трунцевский отмечает, что законодатель правильно распределяет ответственность с учетом наступления последствий, однако не устанавливает правил по определению размера тяжести такого вреда, оставляя данный вопрос на стороне судебной системы [20, с. 103]. Как уже указывалось, законотворческий подход, предусматривающий неконкретизированные общественно опасные последствия преступлений в сфере компьютерной информации, представляется некорректным, не учитывающим положения федерального закона от 26 июля 2017 г. № 187-ФЗ. Целесообразно заменить признак «вред КИИ РФ» на признак «компьютерный инцидент», при этом оставив другие элементы диспозиции без изменений.

С субъективной стороны составы преступления, описанные в ч. 1 и 2 ст. 274.1 УК РФ, характеризуются виной в форме умысла. Причем признак «заведомо предназначенных», как нам кажется, указывает на возможность только прямого умысла. Преступление, предусмотренное ч. 3 ст. 274.1 УК РФ, может быть совершено и умышленно, и по неосторожности. Это обусловлено тем, что нарушения режима функционирования автоматизированных систем управления могут быть следствием ошибок в работе систем или результатом целенаправленного воздействия [там же, с. 105].

Ни в один из составов, в том числе квалифицированных, законодатель не включил признаки мотива или цели в качестве конститутивных или отягчающих. Причины такого решения представляются не вполне ясными, ведь подобный подход уже используется по отношению к регулированию иных компьютерных преступлений. Так, в ст. 272 и 273 УК РФ предусмотрен признак «совершенное из корыстной заинтересованности», который в судебно-следственной практике встречается достаточно часто. Очевидно, что посягательства на КИИ РФ совершаются по различным мотивам, и корыстный не последний из них. Кроме того, неоднородными являются также цели преступления: одни из них увеличивают степень его общественной опасности, а другие — нет. Разумным видится высказанное в науке уголовного права мнение о том, что отсутствие в законе прямого указания на обязательность анализа мотивов и целей компьютерных преступлений представляет собой пробел законодательства [21, с. 155].

На наш взгляд, целесообразно закрепить в качестве квалифицирующих признаков такие внутренние побуждения и цели, которые являются распространенными и повышающими степень общественной опасности деяния одновременно. Современные компьютерные атаки, как правило, совершаются не из хулиганских мотивов, а имеют в основе конкретные потребности человека, вызывающие решимость совершить преступле-

ние. Было бы разумно учесть этот факт при дифференциации уголовной ответственности.

Как отмечается в научной литературе, наиболее распространенными мотивами компьютерных атак являются: финансовая выгода (корысть), желание завладеть определенными данными, хактивизм и мотивы, связанные с ведением кибервойны [22]. Именно корыстные побуждения должны, на наш взгляд, учитываться в качестве квалифицирующего признака в ст. 274.1 УК РФ. Основаниями для этого служат не только их распространенность, но и тот факт, что корыстный мотив подчеркивает устойчивость и закономерность противоправных стремлений, характеризует личность преступника с отрицательной стороны, и в этом смысле увеличивает степень опасности деяния и лица, его совершившего. К тому же в иных компьютерных преступлениях данное внутреннее побуждение уже учтено (ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ).

В то же время хотелось бы обратить внимание на использование в уголовном законе терминов «заинтересованность», «мотив» и «побуждение», которые в действительности имеют одинаковое значение. Все они характеризуют некие внутренние процессы деятельности человека, вызывающие решимость совершить преступление. Необходимость сведения различных терминов, имеющих одинаковое смысловое значение, к одному целому является очевидной. В рамках данной работы мы ограничимся лишь тем, что корыстный мотив стоит закрепить в ст. 274.1 УК РФ в качестве квалифицирующего признака. При этом желательно использовать юридическую конструкцию «из корыстных побуждений» как в данном случае, так и во всех главах УК РФ.

Имеют важное значение направленность общественно опасного деяния и предполагаемый преступником результат. Как показало ранее проведенное нами исследование, значительная часть киберпреступлений направлена на совершение иных противоправных деяний. То есть образуется цепочка деликтов, при которой компьютерное преступление выступает предикатным для дальнейших деликтов [23]. Изучение судебной практики по делам о неправомерном воздействии на КИИ РФ позволило нам сделать вывод о том, что данное общественно опасное деяние в определенных случаях действительно совершается с целью скрыть другое преступление или облегчить его совершение.

В частности, как следует из приговора Пролетарского районного суда г. Твери от 21 апреля 2022 г. по делу № 1-56/2022, Б. Д. Е. был трудоустроен в ПАО «ВымпелКом» (субъект КИИ РФ) на должность специалиста. Для исполнения служебных обязанностей виновному лицу предоставлялся доступ к ресурсам и техническим средствам, в том числе ИТ-оборудованию — автоматизированной системе расчетов Amdocs Ensemble. В августе 2020 г. Б. Д. Е. решил совершить хищение денежных средств ПАО «ВымпелКом» путем подключения скидок абонентам сотовой связи, о чем сообщил соучастнице Е. Е. В. В нарушение установленных требований Б. Д. Е. через программный модуль ACRM путем модификации компьютерной информации, а также иного вмешательства в функционирование средств хранения обработки и передачи компьютерной информации, произведя корректировки лицевых счетов, незаконно осуществил оформление услуги «50%-ная скидка на абонентскую плату» и возвраты денежных средств на основной баланс абонентских номеров, предоставленных Е. Е. В. В дальнейшем Е. Е. В. перевела часть похищенных денежных средств на банковскую карту Б. Д. Е.[7]

Цель скрыть другое преступление или облегчить его совершение не является новой для отечественного уголовного права. Она включена в перечень обстоятельств, отягчающих наказание (п. «е.1» ч. 1 ст. 63 УК РФ), а также выступает квалифицирующим признаком отдельных составов преступлений (например, в составе, предусмотренном ч. 4 ст. 327 УК РФ). Такой подход может вызывать обоснованные возражения в связи с тем, что в определенном смысле закрепляет повторность уголовной ответственности, но мы придерживаемся иной позиции. Цель скрыть другое преступление или облегчить его совершение не может влечь за собой повторность ответственности, поскольку представляет собой признак конкретного деяния. Само же «другое преступление» квалифицируется по отдельной статье, охватывающей отдельные признаки, а значит, является отдельным основанием уголовной ответственности. При этом вышеуказанная цель увеличивает степень общественной опасности деяния, проверена практикой и находит поддержку в литературе. В целом К.Н. Евдокимов [24] и В.Г. Степанов-Егиянц [25] убедительно высказались относительно необходимости установления цели, связанной с

[7] Приговор от 21 апреля 2022 г. по делу № 1-56/2022 по обвинению Б. Д. Е. в совершении преступлений, предусмотренных пп. «а, в» ч. 3 ст. 159.6, ч. 4 ст. 274.1 УК РФ, и Е. Е. В. в совершении преступления, предусмотренного п. «в» ч. 3 ст. 159.6 УК РФ // ГАС «Правосудие».

совершением иных преступлений, в качестве квалифицирующего признака деяний, посягающих на безопасность компьютерной информации.

Изложенное позволяет сделать вывод о том, что признаки субъективной стороны составов преступлений, закрепленных в ст. 274.1 УК РФ, нуждаются в уточнении. В частности, целесообразно учесть отдельные мотивы и цели в качестве квалифицирующих признаков. Среди них можно назвать корыстные побуждения и цель скрыть другое преступление или облегчить его совершение. К сожалению, техническим препятствием к этому является конструкция статьи, включающая сразу несколько самостоятельных составов, как умышленных, так и неосторожных. Для неосторожных составов при этом, как известно, нехарактерно наличие юридически значимых мотивов или целей, поэтому простое включение соответствующих квалифицирующих признаков в ч. 4 или ч. 5 будет противоречить иным положениям уголовного закона.

Данная проблема может быть разрешена как минимум двумя способами. Возможно вынесение всех самостоятельных составов в отдельные статьи с отдельными квалифицирующими признаками, как это сделано в ст. 272, 273 и 274 УК РФ. Либо в ст. 274.1 УК РФ следует выделить дополнительные части, в которых необходимо будет предусмотреть отдельные квалифицированные составы по отношению к каждому из самостоятельных составов, как это сделано, например, в ст. 195 УК РФ.

Выводы

Роль КИИ РФ в обеспечении нормального функционирования государства и общества непременно будет возрастать. При этом ее уголовно-правовая защита нуждается в совершенствовании. Проведенное исследование позволило сформулировать и обосновать направления такого совершенствования.

Как представляется, введение в УК РФ ч. 1 ст. 274.1 не отвечало требованиям криминализации, а ее юридическая конструкция затрудняет деятельность работников судебных и следственных органов. Действующая ст. 273 УК РФ обладает достойным потенциалом для охвата неправомерных создания, распространения и (или) использования каких-либо компьютерных программ в отношении КИИ РФ или информации, содержащейся в ней. Вместо создания специального состава целесообразно было бы скорректировать закрепленные в ст. 273 УК РФ санкции с учетом объекта, предмета и возможных общественно опасных последствий.

Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ раскрывает содержание таких явлений, как компьютерная атака и компьютерный инцидент. Данные понятия являются достаточно полными и конкретными, в отличие от признаков общественно опасного деяния и общественно опасного последствия, закрепленных в ч. 2 ст. 274.1 УК РФ. Введение их в данный состав могло бы поспособствовать лучшему взаимодействию между нормами, регулирующими защиту одинаковых общественных отношений, а также более эффективной работе следственных и судебных органов. Таким образом, думается, что юридическая конструкция ч. 2 ст. 274.1 УК РФ должна охватывать общественно опасное деяние в виде компьютерной атаки, а также общественно опасное последствие в виде компьютерного инцидента. В том же направлении следует совершенствовать ч. 3 ст. 274.1 УК РФ, предусматривающую признак «вред критической информационной инфраструктуре Российской Федерации», который является некорректным, не учитывающим положения федерального закона от 26 июля 2017 г. № 187-ФЗ.

Наконец, целесообразно закрепить в составах неправомерного воздействия на КИИ РФ в качестве квалифицирующих признаков такие внутренние побуждения и цели, которые являются распространенными и повышающими степень общественной опасности деяний одновременно, что позволило бы лучшим образом дифференцировать уголовную ответственность. Как представляется, более высокой степенью общественной опасности обладает деяние, совершаемое из корыстных побуждений, а также с целью скрыть другое преступление или облегчить его совершение. Данные признаки не новы для уголовного права, они уже встречаются среди выявленных деликтов, а мнение об их отягчающем характере неоднократно высказывалось в научной литературе.

Представленные в работе рекомендации, думается, могут повысить эффективность действия ст. 274.1 УК РФ, в том числе в совокупности с другими нормами. В то же время необходимо больше исследований по данной тематике, способных подтвердить сделанные выводы или разработать иные, более действенные направления совершенствования закона.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. Monteith S. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry / S. Monteith, M. Bauer, M. Alda [et al.]. — DOI 10.1007/s11920-021-01228-w // Current psychiatry reports. — 2021. — Vol. 23, № 4. — P. 1–9.

2. Мосечкин И.Н. Искусственный интеллект в уголовном праве: перспективы совершенствования охраны и регулирования / И.Н. Мосечкин. — Киров : Изд-во Вят. гос. ун-та, 2020. — 111 с. — EDN TOXRFS.

3. Бегишев И.Р. Уголовная ответственность за создание и (или) распространение роботов, предназначенных для целей совершения преступлений / И.Р. Бегишев. — DOI 10.22394/2074-7306-2021-1-2-140-148. — EDN NZONZN // Северо-Кавказский юридический вестник. — 2021. — № 2. — С. 140–148.

4. Malik J.K. A Brief Review on Cyber Crime-Growth and Evolution / J.K. Malik, S.A. Choudhury // Pramana Research Journal. — 2019. — Vol. 9, № 3. — P. 242–278.

5. Пучков Д.В. Кибертерроризм как новая угроза / Д.В. Пучков. — EDN PZEHVT // Виктимология. — 2021. — Т. 8, № 4. — С. 382–391.

6. Lee K. The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd / K. Lee, J. Lim. — DOI 10.3837/tiis.2016.02.023 // KSII Transactions on Internet and Information Systems (TIIS). — 2016. — Vol. 10, № 2. — P. 857–880.

7. Critical Infrastructure Security and Resilience. Theories, Methods, Tools and Technologies / ed. D. Gritzalis, M. Theoharidou, G. Stergiopoulos. — Cham : Springer, 2019. — 313 p. — DOI 10.1007/978-3-030-00024-0.

8. Qi A. Assessing China's cybersecurity law / A. Qi, G. Shao, W. Zheng. — DOI 10.1016/j.clsr.2018.08.007 // Computer Law & Security Review. — 2018. — Vol. 34, № 6. — P. 1342–1354.

9. Горелик В.Ю. О безопасности критической информационной инфраструктуры Российской Федерации / В.Ю. Горелик, М.Ю. Безус. — EDN SZQXFS // StudNet. — 2020. — Т. 3, № 9. — С. 1438–1448.

10. 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. — EDN HYLLOE // Вестник Ярославского государственного университета им. П.Г. Демидова. Сер.: Гуманитарные науки. — 2019. — № 4. — С. 49–52.

11. Бражник С.Д. Технико-юридический анализ нормы о неправомерном воздействии на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) / С.Д. Бражник, И.А. Пилясов. — EDN MPSAAU // Евразийское Научное Объединение. — 2019. — № 8-3. — С. 198–201.

12. Власов В.А. Некоторые проблемные аспекты неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации / В.А. Власов, Д.А. Михеев. — DOI 10.47643/1815-1337_2020_11_182. — EDN RUOLVT // Право и государство: теория и практика. — 2020. — № 11 (191). — С. 182–185.

13. Авдалян М.Э. Основание криминализации / М.Э. Авдалян. — EDN UAPTYL // Вестник Удмуртского университета. Сер.: Экономика и право. — 2015. — № 3. — С. 139–144.

14. Федосеев Л.И. Анализ отдельных положений статьи 274.1 Уголовного кодекса Российской Федерации / Л.И. Федосеев. — EDN TSEZUV // Законность и правопорядок: история, современность, актуальные проблемы : материалы IV межвуз. студ. науч. конф. — Москва, 2020. — С. 190–194.

15. Дремлюга Р.И. Критическая информационная инфраструктура как предмет преступного посягательства / Р.И. Дремлюга, С.С. Зотов, В.Ю. Павлинская. — DOI 10.24866/1813-3274/2019-2/130-139. — EDN MMQOOR // Азиатско-Тихоокеанский регион: экономика, политика, право. — 2019. — Т. 21, № 2. — С. 130–139.

16. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации : дис. ... д-ра юрид. наук : 12.00.08 / Е.А. Русскевич. — Москва, 2020. — 521 с. — EDN IXNSFI.

17. Крюков Д.В. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: уголовно-правовой аспект / Д.В. Крюков. — EDN NHAUYD // XXV юбилейные Царскосельские чтения : материалы междунар. науч. конф. — Санкт-Петербург, 2021. — С. 308–314.

18. Zeebaree S.R. Impact analysis of SYN flood DDoS attack on HAProxy and NLB cluster-based web servers / S.R. Zeebaree, K. Jacksi, R.R. Zebari. — DOI 10.11591/ijeecs.v19.i1.pp505-512 // Indonesian Journal of Electrical Engineering and Computer Science. — 2020. — Vol. 19, № 1. — P. 510–517.

19. Spam transaction attack detection model based on GRU and WGAN-div / J. Yang, T. Li, G. Liang [et al.]. — DOI 10.1016/j.comcom.2020.07.031 // Computer Communications. — 2020. — Vol. 161, iss. 2. — P. 172–182.

20. Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов / Ю.В. Трунцевский. — DOI 10.12737/art_2019_5_9. — EDN KRNLWX // Журнал российского права. — 2019. — № 5. — С. 99–106.

21. Евдокимов К.Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты / К.Н. Евдокимов. — Иркутск : Изд-во Иркут. юрид. ин-та (филиала) Акад. Генер. прокуратуры РФ, 2016. — 267 с. — EDN YNINGZ.

22. Груздева Л.М. Транспорт как субъект критической информационной инфраструктуры / Л.М. Груздева. — EDN LVLRAB // Транспортное право и безопасность. — 2021. — № 1. — С. 157–163.

23. Мосечкин И.Н. Уголовная ответственность за организацию устойчивой группы лиц, созданной для совершения преступлений в сфере компьютерной информации / И.Н. Мосечкин. — DOI 10.21638/spbu14.2022.102. — EDN DCICHQ // Вестник Санкт-Петербургского университета. Право. — 2022. — Т. 13, № 1. — С. 28–45.

24. Евдокимов К.Н. Субъективная сторона неправомерного доступа к компьютерной информации / К.Н. Евдокимов. — EDN OJQIFH // Вестник Академии Генеральной прокуратуры Российской Федерации. — 2009. — № 4 (12). — С. 53–58.

25. Степанов-Егиянц В.Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект) : дис. ... д-ра юрид. наук : 12.00.08 / В.Г. Степанов-Егиянц. — Москва, 2016. — 389 с.

REFERENCES

1. Monteith S., Bauer M., Alda M., Geddes J., Whybrow P.C., Glenn T. Increasing Cybercrime since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, 2021, vol. 23, no. 4, pp. 1–9. DOI: 10.1007/s11920-021-01228-w.

2. Mosechkin I.N. *Artificial Intelligence in Criminal Law: Prospects of Improving Protection and Regulation.* Kirov, Vyatka State University Publ., 2020. 111 p. EDN: TOXRFS.

3. Begishev I.R. Criminal Liability for the Creation and (or) Distribution of Robots Intended for the Purpose of Committing Crimes. *Severo-Kavkazskii yuridicheskii vestnik = North Caucasus Legal Vestnik*, 2021, no. 2, pp. 140–148. (In Russian). EDN: NZONZN. DOI: 10.22394/2074-7306-2021-1-2-140-148.

4. Malik J.K., Choudhury S.A. A Brief Review on Cyber Crime-Growth and Evolution. *Pramana Research Journal*, 2019, vol. 9, no. 3, pp. 242–278.

5. Puchkov D.V. Cyberterrorism as a New Threat. *Viktimologiya = Victimology*, 2021, vol. 8, no. 4, pp. 382–391. (In Russian). EDN: PZEHVT.

6. Lee K., Lim J. The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd. *KSII Transactions on Internet and Information Systems* (*TIIS*), 2016, vol. 10, no. 2, pp. 857–880. DOI: 10.3837/tiis.2016.02.023.

7. Gritzalis D., Theoharidou M., Stergiopoulos G. (eds.). *Critical Infrastructure Security and Resilience. Theories, Methods, Tools and Technologies.* Cham, Springer, 2019. 313 p. DOI: 10.1007/978-3-030-00024-0.

8. Qi A., Shao G., Zheng W. Assessing China's Cybersecurity Law. *Computer Law & Security Review*, 2018, vol. 34, no. 6, pp. 1342–1354. DOI: 10.1016/j.clsr.2018.08.007.

9. Gorelik V.Yu., Bezus M.Yu. About Security of Critical Information Infrastructure of the Russian Federation. *Student*, 2020, vol. 3, no. 9, pp. 1438–1448. (In Russian). EDN: SZQXFS.

10. Kruglikov L.L., Solovyev O.G., Brazhnik S.D. Responsibility for Unlawful Impact on the Critical Information Infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation) in the System of Economic and Information Security of the State. *Vestnik Yaroslavskogo gosudarstvennogo universiteta im. P.G. Demidova. Seriya: Gumanitarnye nauki = Bulletin of Yaroslavl State University named after P.G. Demidov. Series: the Humanities*, 2019, no. 4, pp. 49–52. (In Russian). EDN: HYLLOE.

11. Brazhnik S.D., Pilyasov I.A. Technical Legal Analysis of the Unlawful Impact on Critical Information Infrastructure of the Russian Federation (Art. 274.1 of the Criminal Code of the Russian Federation). *Evraziiskoe Nauchnoe Ob"edinenie = Eurasian Scientific Association*, 2019, no. 8-3, pp. 198–201. (In Russian). EDN: MPSAAU.

12. Vlasova V.A., Mikneev D.A. Some Problematic Aspects of Undue Influence on the Critical Information Infrastructure of the Russian Federation. *Pravo i gosudarstvo: teoriya i praktika = Law and State: The Theory and Practice*, 2020, no. 11, pp. 182–185. (In Russian). EDN: RUOLVT. DOI: 10.47643/1815-1337_2020_11_182.

13. Avdalyan M.E. Grounds for Criminalization. *Vestnik Udmurtskogo universiteta. Seriya: Ekonomika i pravo = Bulletin of Udmurt University. Series: Economics and Law*, 2015, no. 3, pp. 139–144. (In Russian). EDN: UAPTYL.

14. Fedoseev L.I. Analysis of Separate Clauses in 274.1 Article of the Criminal Code of the Russian Federation. *Legality and Legal Order: History, Modernity, Topical Problems. Materials of the IV Interuniversity Student Scientific Conference*. Moscow, 2020, pp. 190–194. (In Russian). EDN: TSEZUV.

15. Dremlyuga R.I., Zotov S.S., Pavlinskaya V.Y. Critical Information Infrastructure as Object of a Criminal Offence. *Aziatsko-Tikhookeanskii Region: Ekonomika, Politika, Pravo = The Pacific Rim: Economics, Politics, Law*, 2019, vol. 21, no. 2, pp. 130–139. (In Russian). EDN: MMQOOR. DOI: 10.24866/1813-3274/2019-2/130-139.

16. Russkevich E.A. *Differentiation of Liability for Crimes Committed with the Use of Information-communication Technologies and the Issues of their Qualification. Doct. Diss.* Moscow, 2020. 521 p. EDN: IXNSFI.

17. Kryukov D.V. Unlawful Impact on Critical Information Infrastructure of the Russian Federation: Criminal Law Aspect. *XXV Anniversary Tsarskoselsky Readings. Materials of International Scientific Conference*. Saint Petersburg, 2021, pp. 308–314. (In Russian). EDN: NHAUYD.

18. Zeebaree S.R., Jacksi K., Zebari R.R. Impact Analysis of SYN Flood DDoS Attack on HAProxy and NLB Cluster-based Web Servers. *Indonesian Journal of Electrical Engineering and Computer Science*, 2020, vol. 19, no. 1, pp. 510–517. DOI: 10.11591/ijeecs.v19.i1.pp505-512.

19. Yang J., Li T., Liang G., Wang Yu., Gao T.Yu., Zhu F.D. Spam Transaction Attack Detection Model Based on GRU and WGAN-div. *Computer Communications*, 2020, vol. 161, iss. 2, pp. 172–182. DOI: 10.1016/j.comcom.2020.07.031.

20. Truntsevsky Yu.V. Unlawful Impact on Critical Information Infrastructure: Criminal Liability of its Owners and Operators. *Zhurnal rossiiskogo prava = Russian Law Journal*, 2019, no. 5, pp. 99–106. (In Russian). EDN: KRNLWX. DOI: 10.12737/art_2019_5_9.

21. Evdokimov K.N. *Counteracting Computer Crimes in the Russian Federation: Criminological and Criminal Law Aspects.* Irkutsk Law Institute (branch) of the Academy of the Prosecutor General's Office of the Russian Federation Publ., 2016. 267 p. EDN: YNINGZ.

22. Gruzdeva L.M. Transport as a Subject of Critical Information Infrastructure. *Transportnoe pravo i bezopasnost = Transport Law and Security*, 2021, no. 1, pp. 157–163. (In Russian). EDN: LVLRAB.

23. Mosechkin I.N. Criminal Liability for Organizing a Stable Group of Persons Aimed at Committing Crimes in the Field of Computer Information. *Vestnik Sankt-Peterburgskogo universiteta. Pravo = Vestnik of Saint-Petersburg University. Law*, 2022, vol. 13, no. 1, pp. 28–45. (In Russian). EDN: DCICHQ. DOI: 10.21638/spbu14.2022.102.

24. Evdokimov K.N. Mental Element of a Crime Regarding an Illegal Access to Data. *Vestnik Akademii General'noi prokuratury Rossiiskoi Federatsii = Bulletin of the Academy of the RF Prosecutor General's Office*, 2009, no. 4, pp. 53–58. (In Russian). EDN: OJQIFH.

25. Stepanov-Egiyants V.G. *Methodological and Legislative Support of Computer Information Security in the Russian Federation (Criminal Law Aspect). Doct. Diss.* Moscow, 2016. 389 p.

ИНФОРМАЦИЯ ОБ АВТОРЕ

Мосечкин Илья Николаевич — доцент кафедры уголовного права, процесса и национальной безопасности Юридического института Вятского государственного университета, кандидат юридических наук, г. Киров, Российская Федерация; e-mail: Weretowelie@gmail.com.

INFORMATION ABOUT THE AUTHOR

Mosechkin, Ilya N. — Ass. Professor, Chair of Criminal Law, Process and National Security, Law Institute, Vyatka State University, Ph.D. in Law, Kirov, the Russian Federation; e-mail: Weretowelie@gmail.com.

ДЛЯ ЦИТИРОВАНИЯ

Мосечкин И.Н. Проблемы уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации / И.Н. Мосечкин. — DOI 10.17150/2500-1442.2023.17(1).22-34. — EDN OLQBCA // Всероссийский криминологический журнал. — 2023. — Т. 17, № 1. — С. 22–34.

FOR CITATION

Mosechkin I.N. Problems of the Criminal Law Protection of Critical Information Infrastructure of the Russian Federation. *Vserossiiskii kriminologicheskii zhurnal = Russian Journal of Criminology*, 2023, vol. 17, no. 1, pp. 22–34. (In Russian). EDN: OLQBCA. DOI: 10.17150/2500-1442.2023.17(1).22-34.