УДК 343.34:004(470)

DOI dx.doi.org/10.24866/1813-3274/2019-2/130-139

Р. И. Дремлюга¹

Дальневосточный федеральный университет, Владивосток, Россия

E-mail: dremluga.ri@dvfu.ru

С. С. Зотов²

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: zotov.ss@dvfu.ru

В. Ю. Павлинская³

Дальневосточный федеральный университет, г. Владивосток, Россия

E-mail: pavlinskaia.viu@students.dvfu.ru

КРИТИЧЕСКАЯ ИНФОРМАЦИОННАЯ ИНФРАСТРУКТУРА КАК ПРЕДМЕТ ПРЕСТУПНОГО ПОСЯГАТЕЛЬСТВА*

Аннотация. Российская Федерация взяла курс на активную цифровизацию экономики, государства и общества. Одной из основных угроз такого интенсивного внедрения использования информационных систем является возрастающий риск кибератак. Информационная инфраструктура неоднородна, и особого внимания заслуживают объекты, имеющие критическое значение для нормального функционирования государства и общества. Такие объекты законодатель определил как объекты критической информационной инфраструктуры (КИИ). В статье рассматривается критическая информационная структура как предмет преступного посягательства. В ходе исследования выявлены недочёты формулирования статьи 274.1 УК РФ, устанавливающей уголовную ответственность за неправомерное воздей-

¹ Роман Игоревич Дремлюга, кандидат юридических наук, доцент Юридической школы, Дальневосточный федеральный университет, г. Владивосток, Россия.

² Сергей Сергеевич Зотов, заведующий лабораторией информационной безопасности Школы естественных наук, Дальневосточный федеральный университет, г. Владивосток, Россия.

³ Павлинская Валерия Юрьевна, студент Школы цифровой экономики, Дальневосточный федеральный университет, г. Владивосток, Россия.

Для цитирования: Дремлюга Р. И., Зотов С. С., Павлинская В. Ю. Критическая информационная инфраструктура как предмет преступного посягательства // Азиатско-Тихоокеанский регион: экономика, политика, право. 2019. № 2. С. 130–139.

* Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (РФФИ) в рамках научного проекта № 18-29-16129.

ствие на критическую информационную инфраструктуру Российской Федерации. В статье 274.1 УК РФ представлены три формы неправомерного посягательства на компьютерные системы и сети: неправомерный доступ, создание и распространение вредоносных программ, нарушение правил эксплуатации компьютерных систем и сетей. Данные деяния уже уголовно наказуемы согласно ст. 272, ст. 273, ст. 274 УК РФ, если совершены против любых компьютерных систем. Таким образом ключевой дефиницией для отграничения ст. 274.1 УК РФ от других составов статей главы 28 УК РФ является «критическая информационная инфраструктура». В работе показано, что установление на практике отношения предмета посягательства к КИИ может вызвать значительные затруднения. Выявлено, что ч. 1. ст. 274.1 УК РФ может быть неправильно квалифицирована, так как большинство вредоносных средств имеют широкий спектр применения и скорее всего могут применяться, в том числе, и против объектов критической инфраструктуры. Авторы приходят к выводу, что относимость объектов информационной инфраструктуры к критической по их отраслевой, структурной, политической ценности без учёта характеристик информации, с которой работает объект, противоречит парадигме цифровизации экономики. В концепции «цифровой экономики» информация – это основная ценность и продукт производства. Следовательно, ключевым фактором, учитываемым при квалификации и назначении наказания, должна являться информация, на которую посягают.

Ключевые слова: критическая информационная инфраструктура, киберпреступность, преступления в сфере компьютерной информации, предмет преступления, квалификация преступных деяний.

R. I. Dremlyuga¹, Far Eastern Federal University, Vladivostok, Russia
E-mail: dremluga.ri@dvfu.ru

S. S. Zotov², Far Eastern Federal University, Vladivostok, Russia
E-mail: zotov.ss@dvfu.ru

V. Yu. Pavlinskaya³, Vladivostok, Russia
E-mail: pavlinskaia.viu@students.dvfu.ru

CRITICAL INFORMATION INFRASTRUCTURE AS OBJECT OF A CRIMINAL OFFENCE

Abstract. The Russian Federation is committed to active digitalization of the economy, state and society. One of the main threats to such intensive implementation of information systems is the increasing risk of cyber attacks. The information infrastructure is heterogeneous; the objects critical to the normal functioning of the state and society deserve special attention. Such objects are defined by the legislator as objects of critical information infrastructure (CII). The article considers a critical information structure as a subject of criminal encroachment. In the course of the research the formulation drawbacks of article 274.1 of the Criminal Code of the Russian Federation establishing criminal liability for illegal influence on the critical information infrastructure of the Russian Federation were revealed. Article 274.1 of the Criminal Code of the Russian Federation presents three forms of illegal encroachment on computer systems and networks illegal access, creation and distribution of harmful programs, violation of rules of operation of computer systems and networks. These acts are already criminally punishable under Art. 272, Art. 273, Art. 274 of the Criminal Code of the Russian Federation if committed against any computer systems. Thus, the key definition for the delimitation of Art. 274.1. of the Criminal Code of the Russian Federation from other articles of Chapter 28 of the Criminal Code of the Russian Federation is «critical information infrastructure». This paper shows that the establishment in practice of the attitude of the object of the encroachment on the CII can cause significant difficulties. It is revealed that part 1. Article 274.1 of the Criminal Code of the Russian Federation can be qualified incorrectly, as the majority of malicious software have a wide range of applications and most likely can also

¹ Roman I. Dremlyuga, PhD in Law, Associate Professor of the Law School, Far Eastern Federal University, Vladivostok, Russia.

² Sergey S. Zotov, Head of the Information Security Laboratory, School of Natural Sciences, Far Eastern Federal University, Vladivostok, Russia.

³ Valeria Y. Pavlinskaya, student of the School of Digital Economics, Far Eastern Federal University, Vladivostok, Russia.

For citing: Dremlyuga R. I., Zotov S. S., Pavlinskaya V. Yu. Critical informational infrastructure as object of a criminal offence // PACIFIC RIM: Economics, Politics, Law. 2019. № 2. P. 130–139.

be used against critical infrastructure objects. The authors come to the conclusion that the relativity of information infrastructure objects to the critical in their sectoral, structural, political value without taking into account the characteristics of computer information with which the object operates contradicts the paradigm of digitalization of the economy. Information is the main value and product in the concept of «digital economy». Therefore, the information that is being encroached upon is the key factor to be taken into account in qualifying and punishing.

Keywords: critical information infrastructure, cybercrime, crimes in the field of computer information, object of crime, qualification of criminal acts.

Как показывает мировая практика, для развития цифровой экономики в Российской Федерации необходимо внедрение новых подходов в регулирование общественных отношений, осуществляемых посредством информационных технологий [8, 9]. При переходе к цифровой экономике происходят принципиальные изменения в структуре всех общественных отношений, их объектно-субъектного состава и условий реализации [6]. Одним из центральных элементов российской государственной политики по созданию условий для устойчивого развития цифровой экономики является обеспечение информационной безопасности государства и общества [4].

В новой модели функционирования государства и общества огромную роль занимают объекты информационной инфраструктуры, так как они обеспечивают устойчивое развитие цифровизации. Следует отметить, что информационная инфраструктура государства неоднородна, и прежде всего необходимо обеспечивать безопасность точек, сбой в работе которых способен существенно повлиять на стабильность функционирования общества и государства. Чаще всего такие узлы информационной инфраструктуры называют «критической информационной инфраструктурой».

Впервые термин критическая инфраструктура был использован в утверждённых Президентом России 3 февраля 2012 г. Основных направлениях государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации [2]. В данном документе критическая инфраструктура определяется как «совокупность автоматизированных систем управления критически важных объектов и обеспечивающих их взаимодействие информационно-телекоммуникационных сетей, предназначенных для решения задач государственного управления, обеспечения обороноспособности, безопасности и правопорядка, нарушение (или прекращение) функционирования которых может стать причиной наступления тяжких последствий» [2]. Указанный до-

кумент официально обозначил принцип особых мер защиты для отдельных объектов информационной инфраструктуры.

В актуальной трактовке дефиниция «критическая информационная инфраструктура» появилась в Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. [5]. Схожее определение даётся в Федеральном законе «О безопасности критической информационной структуры Российской Федерации» [1].

Понимая ценность защиты критической информационной инфраструктуры, законодатель признал посягательства и неправомерное воздействие на неё уголовно наказуемыми. Федеральным законом от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» были внесены изменения в уголовный кодекс Российской Федерации, в котором появилась Статья 274.1. «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Фактически в статье 274.1 УК РФ представлены три формы неправомерного посягательства на компьютерные системы и сети: неправомерный доступ, создание и распространение вредоносных программ, нарушение правил эксплуатации компьютерных систем и сетей. Данные деяния уже уголовно наказуемы, так за неправомерный доступ уголовная ответственность устанавливается ст. 272 УК РФ. Распространение вредоносных программ подлежит уголовной ответственности согласно ст. 273 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей – это, согласно ст. 274 УК РФ, преступление.

Согласно ст. 274.1 УК РФ уголовная ответственность устанавливается за такие же деяния, которые перечислены в ст. 272, 273, 274 УК РФ, но все эти деяния должны быть направлены против объектов критической информационной инфраструктуры. Таким образом, ключевой дефиницией для отграничения ст. 274.1 УК РФ от других составов статей Главы 28 УК РФ является «критическая информационная инфраструктура».

В тексте Уголовного кодекса Российской Федерации не даётся определение термина «критическая информационная инфраструктура». Анализируемые уголовно-правовые нормы, сформулированные в ст. 274.1 К РФ, имеют бланкетный характер, что предполагает обязательное обращение к другому акту. Дефиниция официально определяется другим нормативным актом, специально посвящённым безопасности критической информационной инфраструктуры.

В Федеральном законе от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» даются определения

критической информационной инфраструктуры, объектов критической информационной инфраструктуры и субъектов критической информационной инфраструктуры. Так, критическая информационная инфраструктура определяется в ст. 2 указанного закона как «объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». В свою очередь, среди объектов КИИ могут быть: информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, которые принадлежат субъектам критической информационной инфраструктуры либо используются ими.

Таким образом, законодатель обозначает, что любые компьютерные системы или сети, принадлежащие субъектам категории «субъект критической информационной инфраструктуры», являются объектом критической информационной инфраструктуры.

Федеральный закон № 187-ФЗ также устанавливает критерии категорирования объектов информационной инфраструктуры. Условно критерии могут быть сгруппированы в пять направлений: социальная значимость, политическая значимость, экономическая значимость, экологическая значимость и значимость для безопасности.

Правила категорирования утверждены Постановлением Правительства РФ от 08.02.2018 № 127 (ред. от 13.04.2019) «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [3]. Согласно «правилам», любому объекту в результате категорирования присваивается одна из трёх категорий значимости: от III-й, самой не значимой, до I-й, с высшей значимостью.

Несмотря на то, что по сути категория объекта КИИ косвенно отражает общественную опасность преступного посягательства на определённый объект критической информационной инфраструктуры, в тексте уголовного кодекса это никак не отражено. В ст. 274.1. УК РФ в качестве квалифицирующих признаков традиционно используются тяжесть последствий деяния и формы соучастия.

Некоторые авторы отмечают, что установление на практике отношения предмета посягательства к КИИ может вызвать значительные затруднения [7]. Например, ч. 1 ст. 274.1 УК РФ сформулирована как «создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации». Следует отметить, что большинство вредоносных средств имеют широкий спектр применения и

скорее всего могут применяться, в том числе, и против объектов критической инфраструктуры.

Создание же вредоносных программ именно для посягательства на определённые объекты маловероятно, и предназначение может быть установлено только в случае уникальных свойств киберзащиты. Таким образом, при широкой трактовке «предназначенности» вредоносной программы под действие ст. 274.1 УК РФ будут подпадать практически любые вредоносные программы, так как большинство программ может быть применено против объектов КИИ. При узкой трактовке очень сложно найти средство (вредоносную программу), которое специально разработано под отдельный объект КИИ.

Объект информационной инфраструктуры может быть отнесён к критическому после внесения его в реестр значимых объектов критической информационной инфраструктуры (ст. 8 № 187-ФЗ).

Если оценить эту законодательную конструкцию по определению и отнесению к объектам КИИ с точки зрения Цифровой экономики, то возникает очевидный вопрос: как в цифровом мире, где компьютерные системы и сети так или иначе связаны друг с другом, выделить какой-либо объект или сеть? Провести границу, где начинается одна информационная инфраструктура и заканчивается другая, достаточно сложно.

Основной ценностью в обществе цифровой экономики является «компьютерная информация», а все социальные отношения рассматриваются через призму информационных потоков. Подход ст. 274.1 УК РФ противоречит идеологии работы с данными в цифровом государстве и обществе. Ценность объекта или общественная опасность деяния должна оцениваться с позиции характеристик информации, которую объект информационной инфраструктуры обрабатывает, хранит или защищает. В законе же используется старый подход, когда информация или какой-либо информационный объект искусственно размечен как охраняемый законом или критический.

Подводя итоги, отметим, что объекты критической информационной инфраструктуры действительно требуют особой уголовно-правовой охраны. Концептуально решение о введении в уголовный кодекс статьи, направленной на привлечение к уголовной ответственности лиц, посягающих на объекты информационной инфраструктуры особой значимости, обосновано. Вопросы вызывает определение самого предмета посягательства. Во-первых, при привлечении к уголовной ответственности за разработку вредоносных программ сложно выделить программы, которые заведомо направлены против объектов критической инфраструктуры. Преимущественно для защиты и функционирования объектов критической информационной инфраструктуры используются широко распространённые программные продукты.

Во-вторых, относимость объектов информационной инфраструктуры к критической по их отраслевой, структурной, политической ценности без учёта характеристик информации, с которой работает объект, противоречит парадигме цифровизации экономики. В концепции «цифровой экономики» информация – это основная ценность и продукт производства. Следовательно, ключевым фактором, учитываемым при квалификации и назначении наказания, должна являться информация, на которую посягают. Законодатель пошёл другим путём и просто «окрасил» некоторые объекты информационной инфраструктуры как критические. По мере того как в России будет внедряться цифровая экономика, т. е. развиваться общественные отношения, связанные с оборотом и производством информации, решение, принятое законодателем, всё больше не будет отвечать реальности.

Список литературы

1. О безопасности критической информационной инфраструктуры Российской Федерации : Федеральный закон Российской Федерации от 26 июля 2017 г. № 187-ФЗ. – URL: http://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения: 25.08.2019).
2. Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации : утв. Президентом РФ 3 февраля 2012 г. № 803. – URL: <http://www.scrf.gov.ru/security/information/document113/> (дата обращения: 25.08.2019).
3. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений : постановление Правительства РФ от 8 февраля 2018 г. № 127 : ред. от 13 апреля 2019 г. – URL: <https://www.garant.ru/products/ipo/prime/doc/71776120/> (дата обращения: 25.08.2019).
4. Об утверждении программы «Цифровая экономика Российской Федерации» : распоряжение Правительства РФ от 28 июля 2017 г. № 1632-р. – URL: <http://government.ru/docs/28653/> (дата обращения: 25.08.2019).
5. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 гг. : указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Собрание законодательства Российской Федерации. – 2017. – 15 мая, № 20. – Ст. 2901.
6. Лопатин, В. Н. Информационная безопасность в электронном государстве // Информационное право. – 2018. – № 2. – С. 14–19.
7. Решетников, А. Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской

Федерации (ст. 274.1 УК России) / А. Ю. Решетников, Е. А. Русскевич // Законы России: опыт, анализ, практика. – 2018. – № 2. – С. 51–55.

8. Ali M. A., Hoque M. R., Alam K. An empirical investigation of the relationship between e-government development and the digital economy: the case of Asian countries // Journal of Knowledge Management. – 2018. – Vol. 22, iss. 5. – URL: <https://www.emeraldinsight.com/doi/abs/10.1108/JKM-10-2017-0477> (дата обращения: 25.08.2019).

9. Linkov, I. Governance strategies for a sustainable digital world / I. Linkov, B. D. Trump, K. Poinsatte-Jones. – DOI 10.3390/su10020440 // Sustainability (Switzerland). – 2018. – Vol. 10, iss. 2. – P. 440. – URL: <http://www.mdpi.com/2071-1050/10/2/440/htm> (дата обращения: 25.08.2019).

References

1. *On the security of critical information infrastructure of the Russian Federation: Federal Law of the Russian Federation of July 26, 2017 No. 187-FZ.* Available at: http://www.consultant.ru/document/cons_doc_LAW_220885/ (accessed 25 August 2019). (In Russian).

2. *The main directions of state policy in the field of ensuring the security of automated control systems for production and technological processes of critical infrastructure of the Russian Federation: approved. The President of the Russian Federation on February 3, 2012 No. 803.* Available at: <http://www.scrf.gov.ru/security/information/document113/> (accessed 25 August 2019). (In Russian).

3. *On approval of the Rules for categorizing objects of critical information infrastructure of the Russian Federation, as well as a list of indicators of criteria for the importance of objects of critical information infrastructure of the Russian Federation and their values: Decree of the Government of the Russian Federation of February 8, 2018 No. 127: ed. from April 13, 2019.* Available at: <https://www.garant.ru/products/ipo/prime/doc/71776120/> (accessed 25 August 2019). (In Russian).

4. *On approval of the Digital Economy of the Russian Federation program: Decree of the Government of the Russian Federation of July 28, 2017 No. 1632-p.* Available at: <http://government.ru/docs/28653/> (accessed 25 August 2019). (In Russian).

5. About the Strategy for the development of the information society in the Russian Federation for 2017–2030 : Decree of the President of the Russian Federation of May 9, 2017 No. 203. *Collection of the legislation of the Russian Federation*, 2017, May 15, no. 20, art. 2901. (In Russian).

6. Lopatin V.N. Informatsionnaya bezopasnost' v elektronnom gosudarstve [Information security in the electronic state]. *Informatsionnoe pravo*, 2018, no. 2, pp. 14–19.

7. Reshetnikov A.Yu., Russkevich E.A. Ob ugovnoyi otvetstvennosti za nepravomernoe vozdeistvie na kriticheskuyu informatsionnuyu infrastrukturu Rossiiskoi

Federatsii (st. 274.1 UK Rossii) [On criminal liability for unlawful influence on the critical information infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of Russia)]. *Zakony Rossii: opyt, analiz, praktika*, 2018, no. 2, pp. 51–55.

8. Ali M. A., Hoque M. R., Alam K. An Empirical Investigation of the Relationship Between E-Government Development and the Digital Economy: the Case of Asian Countries. *Journal of Knowledge Management*, 2018, vol. 22, iss. 5. Available at: <https://www.emeraldinsight.com/doi/abs/10.1108/JKM-10-2017-0477> (accessed 25 August 2019).

9. Linkov I., Trump B. D., Poinsatte-Jones K. Governance Strategies for a Sustainable Digital World. *Sustainability (Switzerland)*, 2018, vol. 10, iss. 2. Available at: <http://www.mdpi.com/2071-1050/10/2/440/htm> (accessed 25 August 2019).