УДК 343.2/.7

В июне 2017 года в УК РФ была введена новая специальная норма – статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», описывающая криминальные угрозы объектам критической информационной инфраструктуры и устанавливающая основания уголовной ответственности ее владельцев и эксплуатантов. В настоящей работе рассматривается нормативное содержание информационной среды как совокупности вычислительных и информационных ресурсов, образующих автоматизированную систему управления технологическими процессами критически важных объектов. Перечисляются и кратко характеризуются причины и основания криминализации указанного посягательства, которое является очевидной стратегической угрозой экономической и информационной безопасности России. Авторы указывают, что неопределенность уголовно-правовых предписаний, закрепленных в ст. 274.1, снижает эффективность борьбы с ней. Для решения существующей проблемы особое значение приобретает доктринальное и судебное толкование норм о компьютерных преступлениях, в том числе направленных против критической информационной инфраструктуры страны.

К л ю ч е в ы е с л о в а : уголовная ответственность; преступление; информационная среда; компьютерная безопасность; экономическая безопасность; неправомерный доступ; информация; уничтожение; блокирование; модификация; копирование; нейтрализация средств защиты.

In June 2017, a new special norm - article 274.1 “Unlawful impact on critical information infrastructure of the Russian Federation” was introduced in the Criminal Code of the Russian Federation, which describes criminal threats to objects of critical information infrastructure and establishes the grounds for criminal liability of its owners and operators. The article discusses the normative content of the information environment as a combination of computing and information resources forming an automated process control system for critical objects. The reasons and grounds for the criminalization of this assault, which is an obvious strategic threat to the economic and information security of Russia, are listed and briefly characterized. The authors indicate that the uncertainty of the criminal law provisions enshrined in Art. 274.1 reduces the effectiveness of the fight against it. To solve the existing problem, the doctrinal and judicial interpretation of the rules on computer crimes, including those directed against the critical information infrastructure of the country, is of particular importance.

K e y w o r d s : criminal liability; crime; information environment; computer security; economic security; unlawful access; information; destruction; blocking; modification; copying; neutralization of protective equipment.

Л. Л. Кругликов, О. Г. Соловьев, С. Д. Бражник

Ярославский государственный университет им. П. Г. Демидова
E-mail: krugliko@uniyar.ac.ru
E-mail: olegsol1961@yandex.ru
E-mail: bsd2009@mail.ru

Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в системе экономической и информационной безопасности государства

Научная статья

L. L. Kruglikov, O. G. Solovyev, S. D. Brazhnik

P. G. Demidov Yaroslavl State University

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

Scientific article

По информации заместителя директора Национального координационного центра по компьютерным инцидентам Н. Мурашова, только в 2018 году на Россию было совершено более 4,3 миллиарда кибератак на критическую информационную инфраструктуру (*далее – КИИ*). Семнадцать

тысяч из них были признаны наиболее опасными. В 2017 году их число было почти в два раза меньше (2,4 миллиарда случаев кибератак, 12 тысяч из них признаны наиболее опасными) [1]. По данным, озвученным секретарем Совета Безопасности РФ Н. Патрушевым, в 2017 году было зафиксировано около 52,5 млн кибератак на сайты госорганов (в 2016 году – 14,4 млн). Он отметил, что «защищенность государственных и иных информационных систем от компьютерных атак и средств компьютерной разведки остается недостаточной и в большинстве случаев не отвечает существующим угрозам» [2]. Известное консалтинговое бюро Juniper Research считает, что общие убытки коммерческих компаний от хакерских взломов в 2018 году составили 3 трлн долларов. В свою очередь, финансовые потери российской экономики от кибератак в 2019 г. могут достигнуть колоссальных размеров – 1,6–1,8 трлн рублей, как считает зампред Сбербанка Станислав Кузнецов [3, с. 120].

Очевидно, что такие угрозы экономической и информационной безопасности государства должны иметь правовое реагирование законодателя. Особое место в системе нормативного противодействия противоправным проявлениям в информационной сфере занимает уголовное законодательство. К середине текущего десятилетия стало ясно, что нормы, закрепленные на тот момент в гл. 28 УК РФ «Преступления в сфере компьютерной информации», уже не способны в полной мере обеспечить надлежащую уголовно-правовую охрану информационной среды, средств коммуникации и связи в системе государственного управления, экономике, социальной сфере. Как результат, в связи с нарастанием угроз применения вредных информационных технологий и в целях безопасности функционирования информационных и телекоммуникационных систем критически важных объектов инфраструктуры законодатель в 2017 году криминализировал неправомерное воздействие на КИИ РФ (ст. 274.1 УК).

Не сомневаясь в целесообразности усиления охраны критически важных объектов (военные объекты, предприятия, обеспечивающие жизнеобеспечение целых территорий, объекты энергетики (в первую очередь атомной), транспорт, в первую очередь воздушный и т. д.), в том числе и объектов КИИ РФ, анализ нормы дает основание утверждать, что законодатель сделал это с определенными погрешностями. С полным основанием эту норму можно отнести к категории так называемых «мертворожденных», «которые изначально в момент своего создания и закрепления в законе не могли претендовать на широкое применение; качество и культура технического оформления нормы, при котором, возможно, объективно необходимый запрет конструируется таким образом, что лишает правоприменителя возможности не только применять, но и адекватно понимать содержание нормы» [4, с. 8].

Совершенно не случайно поэтому, как нам представляется, несмотря на динамичный рост числа киберпреступлений в мире и неимоверное количество компьютерных атак на отечественные объекты, количество лиц, ежегодно привлекаемых к уголовной ответственности в России за совершение в сфере компьютерной информации, остается незначительным. Количество же осужденных по ст. 274.1 УК, по данным Судебного департамента при Верховном суде РФ, за 2018 года равно нулю [5]. Заметим, что негативное влияние на правоприменительную практику по делам о компьютерных преступлениях оказывает отсутствие специальных разъяснений Пленума ВС РФ по дискуссионным аспектам квалификации деяний, закрепленных в гл. 28 УК РФ [6].

Во-первых следует обратить внимание на чрезмерно широкое, на наш взгляд, законодательное формулирование объектов КИИ, где указывается, что, кроме собственно КИИ объекта, сюда входят сети электросвязи, например, и другие информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры [7]. Если следовать логике законодателя, то под объектами КИИ следует понимать некий технологический комплекс, включающий в том числе и строения – хранилища информации, сети электрические, сети электросвязи, используемые для организации взаимодействия таких объектов. Это дает основание считать объектами КИИ все, что их «окружает» (электрические сети, сети электросвязи; автоматизированные системы управления субъектов критической информационной инфраструктуры). В итоге мы «выйдем» на то, что у нас почти все отрасли без исключения и даже предприятия, их обеспечивающие (например, электроэнергией, связью), будут влиять на национальную безопасность, обороноспособность и выживаемость страны.

Во-вторых, настораживает законодательное формулирование субъектов КИИ [7], из которого следует, что субъектами КИИ могут быть не только органы государственной власти, организации

и учреждения государственной власти и субъектов Российской Федерации: МО РФ, МИД РФ, все правоохранительные органы, банковская система, – но и иные **юридические лица** и **индивидуальные предприниматели**, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности или которые обеспечивают взаимодействие указанных систем или сетей. Такой круг субъектов КИИ даже представить сложно, тем более организовать какое-либо эффективное управление или взаимодействие. При этом уполномоченным в области обеспечения безопасности КИИ определена Федеральная служба по техническому и экспортному контролю со штатной численностью чуть больше 1.000 человек.

В-третьих, следует заметить, что ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» предусматривает категорирование всех объектов в зависимости от социальной, политической, экономической значимости, а также значимости объекта КИИ для обеспечения обороны страны, безопасности государства и правопорядка. Во исполнение этого положения принят ряд нормативных актов. Это дает основание утверждать, что некоторые из объектов КИИ более важные, другие – менее важные. Из контекста обозначенных документов следует, что КИИ по категории значимости может быть не только первой, второй и третьей, но и без таковой, т. е. при «отсутствии необходимости присвоения ему одной из таких категорий» [8]. Отсюда очевидно, что, исходя из буквального толкования уголовного закона, все без исключения объекты КИИ нуждаются в уголовно-правовой защите. Действующая редакция ст. 274.1 УК не учитывает данное деление, что представляется существенным упущением с точки зрения дифференциации уголовной ответственности.

Вполне очевидным, на наш взгляд, является нарушение и межотраслевой дифференциации ответственности в случае неправомерного оборота КИИ без соответствующей категории. В настоящее время на Федеральном портале нормативных правовых проектов 26 марта 2019 года размещено уведомление о начале разработки проекта федерального закона о внесении изменений в КоАП РФ в части установления ответственности за нарушение требований по обеспечению безопасности объектов КИИ в случае, когда имело место несоблюдение указанных требований, но оно не повлекло неправомерного воздействия на КИИ. Следует напомнить, что ч. 1 ст. 274.1 УК сформулирована законодателем по типу формальных составов и поэтому не предполагает наступления каких-либо последствий.

В-четвертых, возникает закономерный вопрос о необходимости создания условий для эффективной защиты КИИ и своевременного выявления и пресечения посягательств на информационную среду. Известно только то, что, согласно информации заместителя начальника Управления ФСТЭК России Е. Б. Торбенко, за период действия 187-ФЗ было подано всего 2 000 форм уведомлений о результатах категорирования объектов КИИ (из более 29 000 объектов, подлежащих категорированию), из которых 630 возвращены субъектам КИИ с замечаниями. В 2019 г. процесс категорирования планируют завершить и перейти к следующему этапу – построению системы безопасности [9]. Исходя из сказанного следует, что круг субъектов КИИ до сих пор не определен, несмотря на то что норма уголовного закона (ст. 274.1) вступила в силу с 1 января 2018 года.

Настораживает еще и то, что в соответствии с законодательством и нормативными актами, регулирующими оборот КИИ, следует, что субъекты КИИ на основе установленных показателей критериев значимости и их значений **самостоятельно** определяют категорию принадлежащих им объектов КИИ. Учитывая столь неопределенный круг субъектов и то, что это связано с дополнительными существенными расходами, процесс категорирования КИИ и внесения в соответствующий Реестр может затянуться. Думается, что круг субъектов КИИ должен быть существенно ограничен.

После всего сказанного возникает достаточно много вопросов, первыми из которых являются следующие: объем финансовых затрат ФСТЭК, источники финансирования, оценка качества законодательства о КИИ. Не следует забывать, что возможности уголовного воздействия определяются не только количеством и качеством статей в Уголовном кодексе, но и количеством, а главное качеством имеющегося ресурсного обеспечения

и иноотраслевого права. При совершенствовании уголовного законодательства можно «замахиваться» только на те задачи, до реализации которых мы «доросли» в финансово-экономическом, организационном, аналитическом, научно-методическом, кадровом, нормативном и пропагандистском обеспечении. Как бы это ни звучало парадоксально, но на данный момент сложилась правовая ситуация, в которой виновное лицо подлежит уголовной ответственности за совершение деяния, не имеющего четких границ и критериев его установления. В исследуемом информационном законодательстве и нормативной базе, принятой на его основании, что ни слово, то бесконечные вопросы. Определения, которые допустимы (или приемлемы) в информационном законодательстве и в общем не вызывают особых разночтений у специалистов в области информационных технологий, как правило, слабо пригодны в уголовном законе и правоприменительной практике [10, с. 52].

Как следует из Доктрины информационной безопасности, утвержденной Президентом РФ, состояние информационной безопасности является одной из составляющих национальной безопасности. К сожалению, это лишь теоретическая посылка, законодательно не подкрепленная. В статье 2 УК, как известно, перечислены объекты уголовно-правовой охраны. Информационная сфера там отсутствует. Таким образом, ни информационная, ни компьютерная безопасность не названы в числе объектов уголовно-правовой охраны. Можно, конечно, сказать, что информационная безопасность опосредованно включена в объект гл. 24 УК РФ. Однако думается, что ст. 2 УК РФ следует дополнить новым самостоятельным объектом уголовно-правовой охраны – информационной безопасностью.

По вполне понятным причинам мы обратили внимание лишь на некоторые из проблем, связанных с уголовно-правовой охраной КИИ, поскольку объем настоящей публикации не позволяет претендовать на всестороннее и полное освещение проблемы правотворческих ошибок, допущенных законодателем, доскональный и обстоятельный юридический анализ.

Ссылки

1. Захарова Л. За год на Россию было совершено более четырех миллиардов кибератак. URL: https://rg.ru/2018/12/12/za-god-na-rossiiu-bylo-sovershenо-bolee-chetyreh-milliardov-kiberatak.html (дата обращения: 25.08.2019).

2. Информационная безопасность Российской Федерации: современные угрозы и правовое противодействие. URL: https://www.interfax.ru/russia/552174 (дата обращения: 25.08.2019).

3. Гребеньков А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава // Lex Russica. 2018. № 4 (137). С. 108–120.

4. Бабаев М., Пудовочкин Ю. «Мертвые» нормы в уголовном кодексе: проблемы и решения // Уголовное право. 2010. № 6. С. 4–10.

5. Официальный сайт Судебного департамента при Верховном суде Российской Федерации. Отчет о видах наказания по наиболее тяжкому преступлению (без учета сложения) за 2018 год. URL: http://www.cdep.ru/index.php?id=79&item=4759 // (дата обращения: 25.08.2019).

6. Князьков А. А. Новое Постановление Пленума Верховного Суда РФ об освобождении от уголовной ответственности: критический анализ основных положений и оценка правоприменительных перспектив // Вестник Ярославского государственного университета им. П. Г. Демидова. Серия Гуманитарные науки. 2013. № 4. С. 73–75.

7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры» // Российская газета. 2017. 31 июля.

8. Информационное письмо от 24 августа 2018 г. № 240/25/3752 «По вопросам представления перечней объектов критической информационной инфраструктуры, подлежащих категорированию, и направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий». URL: https://fstec.ru/component/attachments/download/2006 (дата обращения: 25.08.2019).

9. ИБКВО 2019. Е. Торбенко. ФСТЭК: О категорировании объектов. URL: http://json.tv/ict_video_watch/ibkvo-2019-elena-torbenko-fstek-bolee-29-tysyach-obektov-kategorirovaniya-napravleny-nam-20190319030955 (дата обращения: 25.08.2019).

10. 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. С. 51– 55.