О СОВЕРШЕНСТВОВАНИИ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ОБ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ

МАЛЫГИН
Иван Игоревич

консультант отдела государственной регистрации нормативных правовых актов в социальной и культурной сферах Департамента регистрации ведомственных нормативных правовых актов Министерства юстиции РФ (г. Москва)

aspugpravo@yandex.ru

https://doi.org/10.33874/2072-9936-2021-0-3-118-122

В теории уголовного права высказываются довольно обстоятельные нарекания относительно конструкции уголовно-правовой нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру РФ. В связи с этим формулируются предложения по внесению изменений в ст. 274[1] Уголовного кодекса РФ (далее – УК РФ). Цель исследования состоит в разработке и научном обосновании рекомендаций по преодолению проблем, связанных с законодательным определением ответственности за неправомерное воздействие на критическую информационную инфраструктуру РФ. Реализация указанной цели достигалась путем оценки состояния отечественного уголовного законодательства (ст. 274[1] УК РФ) и изучения имеющихся точек зрения в доктрине уголовного права. Исследование основано на применении общенаучных и специальных методов (анализ, синтез, индукция, формально-юридический, абстрактно-логический и др.). Проведенное исследование позволило сделать общий вывод о том, что совершенствование отечественного уголовного законодательства об ответственности за неправомерное воздействие на критическую информационную инфраструктуру РФ должно осуществляться по двум основным направлениям: 1) путем совершенствования дифференциации ответственности за неправомерное воздействие на критическую информационную инфраструктуру РФ; 2) посредством установления ответственности за нарушение требований в области безопасности критической информационной инфраструктуры РФ в рамках специальной нормы (ст. 274[2] УК РФ).

Уголовное право; информационная безопасность; компьютерные преступления; объект критической информационной инфраструктуры

Ivan I. MALYGIN

Consultant, Department of State Registration of Normative Legal Acts in the Social and Cultural Spheres, Department for Registration of Departmental Normative Legal Acts of the Ministry of Justice of the Russian Federation (Moscow)

aspugpravo@yandex.ru

ON IMPROVING THE CRIMINAL LEGISLATION ON LIABILITY FOR UNLAWFUL IMPACT ON CRITICAL INFRASTRUCTURE RUSSIAN FEDERATION

In the theory of criminal law, rather detailed criticism is expressed regarding the construction of the criminal law norm on responsibility for unlawful impact on the critical information infrastructure of the Russian Federation. In this regard, proposals are being formulated to amend Article 274[1] of the Criminal Code of the Russian Federation. The purpose of the study is to develop and scientifically substantiate recommendations for overcoming the problems associated with the legislative definition of responsibility for unlawful impact on the critical information infrastructure of the Russian Federation. The implementation of this goal was achieved by assessing the state of domestic criminal legislation (Article 274[1] of the Criminal Code of the Russian Federation) and studying the existing points of view in the doctrine of criminal law. The research is based on the application of general scientific and special methods (analysis, synthesis, induction, formal legal, abstract logical, etc.). The study made it possible to draw a general conclusion that the improvement of domestic criminal legislation

Criminal law; information security; computer crimes; object of critical information infrastructure

on liability for unlawful influence on the critical information infrastructure of the Russian Federation should be carried out in two main directions: 1) by improving the differentiation of responsibility for unlawful influence on the critical information infrastructure of the Russian Federation; 2) by establishing responsibility for violation of the security requirements of the critical information infrastructure of the Russian Federation within the framework of a special norm (Article 274² of the Criminal Code of the Russian Federation).

Информационные технологии занимают центральное место в современной коммуникации. Смартфон является одним из главных (если не главным) инструментов человека XXI в. В нем хранится чуть ли не вся жизнь владельца: список личных контактов, переписка, информация о состоянии здоровья, фотографии, сведения об оплате товаров и услуг (с указанием места и времени осуществления расчетов). Однако повсеместно распространена не только цифровая коммуникация. Цифровизация уже в значительной степени изменила бизнес, механизмы государственного и местного (муниципального) управления. Хозяйствующие субъекты и органы власти повсеместно отказываются от бумажного документооборота в пользу жестких дисков и серверов как более удобных и дешевых средств хранения информации. Электронная коммерция последовательно вытесняет традиционную торговлю, автоматизация производства меняет облик современных предприятий – какофония труда сотен и тысяч работников замещается размеренным шумом функционирования роботизированных систем. Сервисы дистанционного банковского обслуживания практически полностью избавили клиента от необходимости личного посещения финансовой организации. В этом же направлении развиваются здравоохранение, образование, сфера оказания услуг и др. С появлением электронной цифровой подписи электронный документооборот получил свое активное развитие и при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, а также при совершении иных юридически значимых действий.

Учитывая экспоненциально возрастающую зависимость человека, общества и государства от компьютерных технологий, нельзя назвать неожиданным рост преступлений, совершаемых с их использованием. Так, по данным ГИАЦ МВД России, в январе–декабре 2020 г. зарегистрировано 510,4 тыс. преступлений, совершенных с использованием компьютерных технологий, что на 73,4% больше, чем за аналогичный период прошлого года. При этом, проводя анализ состояния преступности в РФ за более ранний период (с 2014 по 2019 г.), можно констатировать, что число зарегистрированных преступлений данного вида увеличилось более чем в 25 раз (в 2014 г. было зарегистрировано 11 тыс. преступлений, в 2015 г. – 43,8 тыс., в 2016 г. – 65,9 тыс., в 2017 г. – 90,6 тыс., в 2018 г. – 174,7 тыс., в 2019 г. – 294,4 тыс.).

В отличие от киберинцидентов, затрагивающих отдельных пользователей, компьютерные атаки на информационные инфраструктуры органов власти, коммерческих и иных организаций представляют особую общественную опасность. Это обусловлено рядом обстоятельств. Прежде всего компрометация информационной инфраструктуры организации, как правило, влечет за собой разглашение персональных данных клиентов, сведений, составляющих банковскую и (или) коммерческую тайну. Так, одной из самых крупных утечек данных стал известный инцидент с американской сетью отелей *Starwood*. Злоумышленники в период с 2014 по 2018 г. получили доступ к 383 млн уникальных записей о бронировании – данные, включающие в себя имя, почтовый адрес, электронную почту, дату рождения, пол, в отдельных случаях (порядка 5,3 млн записей) паспортные данные клиентов [1, с. 65]. Помимо этого нельзя не указать и на угрозу прерывания производственного процесса, которое может быть связано не только со значительным имущественным ущербом, но и с прекращением либо ограничением подачи электрической энергии, других источников жизнеобеспечения. О безопасности информационных инфраструктур медицинских организаций, автоматизированных систем управления технологическим процессом в промышленности изначально задумывались весьма мало. Главным параметром надежности считалась отказоустойчивость. Вместе с тем события последних лет кардинально изменили отношение к проблеме. Так, компьютерные атаки на медицинские организации при помощи шифровальщиков наглядно продемонстрировали насколько уязвима система здравоохранения перед современными киберугрозами. Согласно отчету Лаборатории Касперского за 2020 г. антивирусными решениями компании были зафиксированы атаки троянцами-шифровальщиками в отношении 123 630 корпоративных пользователей и 15 940 пользователей, связанных с малым и средним бизнесом [2].

В этом отношении своевременным и важным явилось принятие Федерального закона от 26 июля 2017 г.

№ 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (далее – Федеральный закон № 187-ФЗ), в соответствии с которым госучреждения и компании должны провести работу по оценке и категорированию своих информационных инфраструктур, обеспечить установленный стандартами уровень их программно-технической защиты, а также должны отчитываться об инцидентах уполномоченному ведомству и проходить оценку безопасности.

Федеральным законом от 26 июля 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»» [3] Уголовный кодекс РФ (далее – УК РФ) был дополнен ст. 274[1], предусматривающей ответственность за неправомерное воздействие на объекты критической информационной инфраструктуры РФ.

Появление данной нормы во многом явилось логичным в свете специального выделения специфической группы отношений, связанных с функционированием и охраной критической информационной инфраструктуры РФ. Статистические данные МВД России свидетельствуют о расширении географии применения анализируемой нормы, ее возрастающей востребованности у правоприменителей. Так, если в 2018 г. было зарегистрировано лишь одно преступление (в Камчатском крае), в 2019 г. – 4 (Амурская область – 1, Волгоградская область – 1, Приморский край – 2), а в 2020 г. было зарегистрировано уже 22 преступления (Амурская область – 1, Волгоградская область – 9, Ивановская область – 1, Кемеровская область – 1, Москва – 1, Мурманская область – 1, Пермский край – 1, Приморский край – 3, Республика Северная Осетия-Алания – 1, Республика Татарстан – 1, Республика Хакасия – 1, Тверская область – 1).

Признавая обоснованность проведенной законодателем дифференциации, заметим, что в технико-юридическом плане ее нормативное воплощение нельзя признать оптимальным. При конструировании ст. 274[1] УК РФ допущены серьезные просчеты, которые снижают эффективность уголовно-правового противодействия деяниям, связанным с неправомерным воздействием на критическую информационную инфраструктуру РФ. В теории уголовного права высказываются многочисленные замечания относительно недостатков ее конструкции, которые касаются как формально-юридической определенности криминообразующих признаков, так и реализованной модели дифференциации ответственности.

Изучение имеющихся литературных источников позволяет заключить, что отечественная доктрина уголовного права выказывает довольно обстоятельные нарекания относительно конструкции уголовно-правовой нормы об ответственности за неправомерное воздействие на критическую информационную инфраструктуру РФ. В связи с этим формулируются и обосновываются решения по модернизации ст. 274[1] УК РФ.

Пожалуй, наиболее принципиальным замечанием относительно конструкции ст. 274[1] УК РФ является то, что она не учитывает градацию объектов критической информационной инфраструктуры в зависимости от категории значимости в качестве основания дифференциации уголовной ответственности [4, с. 135; 5, с. 51; 6, с. 55]. Действительно, подобное решение представляется достаточно логичным, поскольку значимость объекта критической информационной инфраструктуры напрямую влияет на степень общественной опасности совершенного в отношении него неправомерного воздействия. В этом отношении исследуемая норма, безусловно, требует доработки. При этом понятно, что все основные составы преступлений, предусмотренные ст. 274[1] УК РФ, будут предполагать совершение посягательства в отношении объектов критической информационной инфраструктуры третьей категории. Дифференциация ответственности будет реализована в зависимости от совершения посягательства на защищенные информационные объекты второй и первой категорий значимости.

В ч. 5 ст. 274[1] УК РФ законодатель дифференцировал ответственность за неправомерное воздействие на критическую информационную инфраструктуру РФ в зависимости от наступления «тяжких последствий». Сама по себе редакция данной части вызывает вопрос в том аспекте, что если в остальных составах компьютерных преступлений законодатель говорит о наступлении таких последствий либо *о создании угрозы их наступления*, то в ч. 5 ст. 274[1] УК РФ говорится только о наступлении тяжких последствий. Видеть здесь какой-то замысел законодателя, на наш взгляд, было бы наивным, как и было бы неискренним попытаться объяснить или оправдать такое решение. Полагаем, что при разработке исследуемой нормы нарушение системности законодателем было допущено по ошибке. В дополнение следует лишь указать, что корректировка анализируемой нормы в данном отношении позволит выдержать системный (блоковый) подход к дифференциации ответственности за совершение преступлений одной группы.

Минэкономразвития России подготовлен законопроект о внесении изменений в ст. 274[1] УК РФ [7]. Главной целью данного документа является устранение формально-юридической неопределенности исследуемой нормы. Так, законопроект предполагает отказ от признака причинения вреда критической информационной инфраструктуре по причине его многозначности, что «детерминирует высокую степень субъективности при его толковании и последующем

применении». Одновременно с этим предлагается включить признак – «причинение крупного ущерба».

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

Федеральный закон № 187-ФЗ в ст. 9 также предусматривает целый ряд принципиально значимых обязанностей субъектов критической информационной инфраструктуры: 1) незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ; 2) оказывать содействие должностным лицам соответствующего федерального органа в обнаружении, предупреждении и ликвидации последствий компьютерных атак; 3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность и др.

Умышленное неисполнение указанных выше обязанностей соответствующими субъектами объективно причиняет или создает угрозу причинения вреда состоянию защищенности критической информационной инфраструктуры РФ. Так, нарушение порядка реагирования на компьютерные инциденты, невыполнение вынесенных предписаний объективно может повлечь наступление тяжких последствий в сфере функционирования информационных объектов особой важности.

При этом положения ст. 274^1 УК РФ либо вовсе не распространяются на случаи умышленного неисполнения соответствующих обязанностей, либо распространяются в крайне незначительной форме. В связи с этим полагаем, что в данном отношении отечественное уголовное законодательство требует совершенствования. Перспективным видится дополнение гл. 28 УК РФ ст. 274^2 «Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации».

В отечественной теории уголовного права данную идею обосновывает Е. А. Русскевич. По мнению автора, установление уголовной ответственности за уклонение от исполнения отдельных обязанностей лицами, ответственными за обеспечение безопасности объектов критической информационной инфраструктуры, может быть реализовано двумя способами: 1) путем построения соответствующего состава с административной; 2) посредством определения состава преступления с материальной конструкцией, включив в качестве криминообразующих признаков причинение крупного ущерба либо наступление тяжких последствий [8, с. 187–190].

В данном аспекте позиция автора представляется дискуссионной. Реализация первой модели потребует внесения соответствующих изменений в отечественный закон об административных правонарушениях. Кроме того, с учетом специфики исследуемого деяния есть основания полагать, что состав с административной преюдицией просто не будет работать – владелец (оператор) объекта критической информационной инфраструктуры РФ будет оперативно менять ответственных исполнителей, тем самым делая невозможным повторность нарушения.

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

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

Пристатейный библиографический список

1. Threat Zone 2019 : Иллюзия безопасности // BI.ZONE : сайт. URL: https://bi.zone/upload/for_download/Threat-Zone_2019_RU.pdf (дата обращения: 16.06.2021).

2. Kaspersky Security Bulletin 2020. Статистика // Лаборатория Касперского : сайт. URL: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_ru.pdf (дата обращения: 16.06.2021).

3. Федеральный закон от 26 июля 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»» // СПС «КонсультантПлюс».

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

5. *Кругликов Л. Л., Соловьев О. Г. Бражник С. Д.* Ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) в системе экономической и информационной безопасности государства // Вестник ЯрГУ. Серия «Гуманитарные науки». 2019. Т. 4. (50).

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

7. Проект федерального закона «О внесении изменений в статью 274[1] Уголовного кодекса Российской Федерации» (подготовлен Минэкономразвития России, ID проекта 04/13/05-20/00102094) // СПС «КонсультантПлюс».

8. *Русскевич Е. А.* О совершенствовании уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации // Уголовное право : стратегия развития в XXI веке : материалы XVIII Международной научно-практической конференции «Уголовное право : стратегия развития в XXI веке» (Москва, МГЮА им. О. Е. Кутафина, 21–22 января 2021 г.). М. : РГ-Пресс, 2021.

References

1. Threat Zone 2019: The Illusion of Security. URL: https://bi.zone/upload/for_download/Threat-Zone_2019_RU.pdf (date of application: 16.06.2021).

2. Kaspersky Security Bulletin 2020. Statistics URL: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_ru.pdf (date of application: 16.06.2021).

3. Federal Law of 26 July 2017 No. 194-FZ "On Amendments to the Criminal Code of the Russian Federation and Article 151 of the Criminal Procedure Code of the Russian Federation in Connection with the Adoption of the Federal Law 'On the Security of the Critical Information Infrastructure of the Russian Federation'" (SPS "ConsultantPlus").

4. *Dremliuga R. I., Zotov S. S., Pavlinskaia V. Iu.* Critical Information Infrastructure as a Subject of Criminal Encroachment. *Asia-Pacific Region: Economics, Politics, Law*. 2019. No. 2.

5. *Kruglikov L. L., Soloviev O. G. Brazhnik S. D.* Responsibility for Unlawful Influence 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. *Bulletin of Yaroslavl State University. Series "Humanities"*. 2019. Vol. 4 (50).

6. *Reshetnikov A. Iu., Russkevich E. A.* On Criminal Liability for Unlawful Influence on the Critical Information Infrastructure of the Russian Federation (Article 2741 of the Criminal Code of Russia). *Laws of Russia: Experience: Analysis, Practice*. 2018. No. 2 (66).

7. Draft Federal Law "On Amendments to Article 2741 of the Criminal Code of the Russian Federation" (prepared by the Ministry of Economic Development of Russia, project ID 04/13/05-20/00102094) (SPS "ConsultantPlus").

8. *Russkevich E. A.* On Improving the Criminal Law Protection of the Critical Information Infrastructure of the Russian Federation. In Criminal Law: Development Strategy in the 21st Century: Materials of the 18th International Scientific and Practical Conference "Criminal Law: Development Strategy in the 21st Century" (Moscow, Kutafin Moscow State Law Academy, 21–22 January 2021). Moscow: RG-Press, 2021.