УГОЛОВНО-ПРАВОВЫЕ РИСКИ СУБЪЕКТОВ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ И ИХ ВЛИЯНИЕ НА ПРОЦЕССЫ ЦИФРОВИЗАЦИИ ОТРАСЛЕЙ НАРОДНОГО ХОЗЯЙСТВА

В. В. КОМАРОВ

преподаватель Автономной некоммерческой организации дополнительного профессионального образования центр повышения квалификации «Академия информационных систем», г. Москва, Российская Федерация

Развитие и внедрение цифровых технологий в различных сферах деятельности государственных и коммерческих организаций приводит не только к ожидаемым положительным изменениям экономики, жизни общества и государства, но и повышает вероятность преступного воздействия на информационную инфраструктуру с нарушением ее работоспособности, что повлечет наступление тяжких негативных последствий в форме значительного ущерба юридическим и физическим лицам, а в отдельных случаях также и государственным интересам в целом [1].

Необходимо отметить, что уже в 1996 году в Уголовном кодексе Российской Федерации была сформирована специальная глава 28 «Преступления в сфере компьютерной информации», включившая в себя уголовные статьи, направленных на криминализацию неправомерного воздействия на информацию [2]. Но дальнейший прогресс информационных технологий, их проникновение (цифровизация) во все сферы экономической деятельности, а особенно опыт ликвидации последствий масштабных компьютерных атак (WannaCry, Nypetya) на государственные корпорации, органы государственной власти, объекты ядерной энергетики Российской Федерации в 2017 году показал необходимость в срочной правовой защите информационной инфраструктуры в целом. В 2018 году вступил в силу не только закон, устанавливающий ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [3], так же вступил в силу закон, внесший изменения в Уголовный и Уголовно-процессуальный кодексы России [4].

Выделение отдельной нормы криминализации нового общественно опасного деяния вызвало неоднозначную реакцию профессионального сообщества, авторами указывалось как поспешность принятых решений, так и несовершенство используемых формулировок [5], [6].

В дальнейшем, правоприменительная практика по ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» была обобщена Судебным департаментом при Верховном суде Российской Федерации [7], проведен анализ и даны разъяснения по квалификации уголовных преступлений в данной сфере [8].

Но в рамках данной работы наибольший интерес представляет квалификация и правовая оценка действия/бездействия персонала организации, отнесенной к субъектам критической информационной инфраструктуры. Судебная практика подтвердила мнение исследователей, сделавших выводы о том, что к уголовной ответственности по данной статье УК РФ будут привлекаться также и работники организаций, обеспечивающих эксплуатацию объектов критической информационной инфраструктуры [9].

В ходе работы было проанализировано 168 судебных решений, размещенных в государственной автоматизированной системе «Правосудие» Судебного департамента при Верховном суде Российской Федерации, охватывающих период с 2019 по 2024 годы и все субъекты Российской Федерации.

Результаты проведенного анализа:

– 86 % решений выносились в отношении работников субъектов КИИ;

– 98 % решений по преступным деяниям работников субъектов КИИ квалифицированы по отягчающей ч.4 ст.274.1 УК РФ («с использованием служебного положения»);

– 72 % решений содержит указание об отсутствии умысла преступника на нанесение вреда критической информационной инфраструктуры.

Следственные органы полагает, а суды соглашаются с тем, что, действия обвиняемых «нарушают целостность», в результате чего, «циркулирующая в объекте КИИ информация теряют объективность, достоверность и актуальность» [10].

Данная позиция следствия полностью совпадает с позицией Генеральной прокуратуры России [11].

Следует отметить, что потеря достоверности и актуальности информации, обрабатываемой в объекте КИИ, наступает не только при умышленном внесение недостоверных данных, но и при ошибочных (случайных) действиях пользователя информационной системы, а также при бездействие – не внесение данных по какой либо причине, либо внесение с задержкой, превышающих время, отведенное эксплуатационной документацией.

При этом, все чаще суды фиксируют решения о неверной квалификации органами следствия и излишне вмененной ст. 274.1 УК РФ при совершении традиционных «не компьютерных» преступлений [12–16].

Более того, судами вынесены обвинительные приговоры о привлечении к уголовной ответственности за тяжкое компьютерное преступление в отношении работников субъектов КИИ, совершенные без использования средств вычислительной техники и без воздействия на компьютерную информацию (за рукописные записи на бумажных носителях) [17], [18].

Отдельной дискуссии заслуживает практика повышения уголовной ответственности для лиц, совершающих преступления с использованием своего служебного положения [19]. Так, практически повсеместно следствием и судами под использованием служебного положения понимается использование учетных записей пользователя информационной системы (логин и пароль), оформленных работодателем для исполнения обвиняемым своих должностных (служебных) обязанностей и/или использование компьютерной техники работодателя, а не выполнение организационно-распорядительных, административно-хозяйственные функций в организации.

Не указание на форму вины в составе нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации является упущением законодателя, поскольку сама конструкция состава логически требует признания возможности совершения деяния по неосторожности, но ч. 2 ст. 24 УК РФ позволяет признавать преступление совершенным по неосторожности, только если это предусмотрено соответствующей статьей Особенной части УК РФ [20].

Учитывая вышеизложенное, а также значительный рост количества уголовных дел по ст.274.1 УК РФ [21], прогнозируется проявление следующих негативных для дальнейшей цифровизации отраслей народного хозяйства факторов:

– дифференцирование наказания работника в зависимости от формы обработки информации в организации. Работник не внес вовремя запись об уборке помещения в график на бумажном носителе – дисциплинарный проступок, работник не внес запись в электронный журнал автоматизированной системы учета уборки – тяжкое компьютерное преступление;

– дифференцирование наказания в зависимости от наличия трудовых отношений преступника с пострадавшей организацией. Отягощение наказания для работника за использование средств вычислительной техники работодателя и/или прав доступа к информационным системам организации.

Таким образом, руководители и работники организаций, которые включаются в программы цифровизации соответствующих отраслей народного хозяйства, будут расценивать внедрение компьютерной техники и современных цифровых решений в своих организациях как угрозу личной безопасности и благополучию.

В свою очередь, учет вышеуказанных негативных факторов требует соответствующей оценки субъектов правотворчества и правоприменения с учетом потребности государства в максимально широком внедрении цифровых технологий.

СПИСОК ЛИТЕРАТУРЫ

1. Голубев, Ф.А. – Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации / Ф.А. Голубев // Право и политика. – 2020. – № 10. – С. 50–59. DOI: 10.7256/2454-0706.2020.10.33985.
2. Лавицкая, М.И., Крапчатова, И.Н. Структурно-содержательная характеристика главы 28 УК РФ: юридико-технические и правореализационные проблемы составов преступлений в сфере компьютерной информации / М.И. Лавицкая, И.Н. Крапчатова // Российский следователь. – 2021. – № 6. – С. 35–41.
3. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4736.
4. Федеральный закон 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» «Собрание законодательства РФ», 31.07.2017, № 31 (Часть I), ст. 4743.
5. 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 // Евразийское Научное Объединение. – 2019. – № 8-3(54). – С. 198–201. – EDN MPSAAU.
6. Густова, Э.В. Новеллы уголовного законодательства: проблемы конструирования и применения / Э.В. Густова // Журнал российского права. – 2018. – № 11. – С. 129–137.
7. «Обзор судебной практики Верховного Суда Российской Федерации № 2 (2023)» (утв. Президиумом Верховного Суда РФ 19.07.2023). «Бюллетень Верховного Суда РФ», № 11, ноябрь, 2023.
8. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет». «Бюллетень Верховного Суда РФ», № 3, март, 2023.
9. Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. – С. 99–106.

10. «О вопросах обоснованности уголовного преследования по статье 274.1 УК РФ» Адвокат Павел Домкин https://www.advodom.ru/practice/advokat-po-ugolovnomu-delu-statya-274-1-uk-rf-php.php.
11. «Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» (утв. Генпрокуратурой России) https://epp.genproc.gov.ru/ru/web/gprf/documents?item=4900252.
12. «Новые схемы кибераферистов и проблема квалификации: судья о развитии цифрового права» Российское агентство правовой и судебной информации (РАПСИ) 21.02.2024 https://rapsinews.ru/digital_law_publication/20240221/309636567.html.
13. Решение Кстовского суда Нижегородской области от 22.02.2024 №1-25/2024.
14. Приговор Вахитовского районного суда г. Казань от 27.12.2024 №1-408/2023.
15. Постановление Каспийского городского суда Республики Дагестан от 18.09.2023 № 1-2/2023.
16. Приговор Центрального районного суда Читы от 30.03.2023 № 1-169/2023.
17. Приговор Прикубанского районного суда Карачаево-Черкесской республики от 05.05.2023 № 1 -11/2023.
18. Приговор Рудничного районного суда города Кемерово Кемеровской области от 23.05.2023 № 1-243/2023.
19. Бычков, В.В., Бражников, Д.А. О концепции отягчающего обстоятельства «совершение преступления с использованием своего служебного положения» / В.В. Бычков, Д.А. Бражников // Российский следователь. – 2019. – № 3. – С. 37–41.
20. Решетников, А.Ю., Русскевич, Е.А. 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.
21. Евдокимов, К.Н. Вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (по материалам судебной практики) / К.Н. Евдокимов // Российский следователь. – 2023. – № 5. – С. 15–19.