Научная статья
УДК 343.34:004.056.5(470)

К ВОПРОСУ ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ (СТ. 274.1 УК РФ)

Андемиркан Борисович Абазов[1], Тимур Аликович Файрушин[2]
[1] Северо-Кавказский институт повышения квалификации (филиал)
Краснодарского университета МВД России, Нальчик, Россия
[2] Уфимский юридический институт МВД России, Уфа, Россия
[1] and-abazov@yandex.ru, [2] fta200483@mail.ru

Аннотация. В настоящей статье авторами дается уголовно-правовая характеристика состава преступления, предусмотренного ст. 274.1 Уголовного кодекса Российской Федерации (неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации).

Ключевые слова: критическая информационная инфраструктура, компьютерная атака, несанкционированный доступ, распространение вредоносного программного обеспечения, обеспечение безопасности, уголовная ответственность.

Для цитирования: Абазов А. Б., Файрушин Т. А. К вопросу об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) // Вестник Уфимского юридического института МВД России. 2023. № 4 (102). С. 86–92.

Original article

ON THE ISSUE OF CRIMINAL LIABILITY FOR UNLAWFUL INFLUENCE ON THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION (ARTICLE 274.1 OF THE CRIMINAL CODE OF THE RUSSIAN FEDERATION)

Andemirkan B. Abazov[1], Timur A. Fayrushin[2]
[1] North Caucasian Institute of Advanced Training (Branch) of Krasnodar University
of the Ministry of Internal Affairs of Russia, Nalchik, Russia
[2] Ufa Law Institute of the Ministry of Internal Affairs of Russia, Ufa, Russia
[1] and-abazov@yandex.ru, [2] fta200483@mail.ru

Abstract. In this article, the authors provide a criminal legal description of the crime provided for in Article 274.1 of the Criminal Code of the Russian Federation (illegal influence on the critical information infrastructure of the Russian Federation).

Keywords: critical information infrastructure, computer attack, unauthorized access, distribution of malicious software, security, criminal liability.

For citation: Abazov A. B., Fayrushin T. A. On the issue of criminal liability for unlawful influence on the critical information infrastructure of the Russian Federation (Article 274.1 of the Criminal Code of the Russian Federation) // Bulletin of Ufa Law Institute of the Ministry of Internal Affairs of Russia. 2023. No. 4 (102). P. 86–92.

Постепенный переход общества к цифровой экономике сопровождается возрастающей ролью информационных технологий, которые находят отражение в развитии са-

мых разных сфер деятельности. Наибольший интерес с этой точки зрения вызывает их применение на объектах, которые относятся к критической информационной инфраструктуре (далее – КИИ).

Для создания стабильно действующей системы КИИ предпринят комплекс соответствующих мер. Так, чтобы обеспечить ее безопасное и полноценное функционирование с защитой от компьютерных атак, был принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ[1], в котором содержится определение понятия КИИ. В соответствии с ч. 6 ст. 2 указанного закона под КИИ следует понимать объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов.

Сфера эксплуатации объектов КИИ весьма обширна, они используются в следующих направлениях:

– медицина и здравоохранение;
– наука и техника;
– транспорт;
– связь;
– финансы и экономика;
– атомная энергетика;
– оборонная промышленность;
– ракетостроение;
– горнодобывающая отрасль;
– металлургия;
– химическое производство.

В Российской Федерации последние годы отмечается существенный рост преступлений в сфере компьютерной информации и деяний, совершенных с использованием информационных технологий. Так, например, если в 2018 г. было зафиксировано 174 674 преступления в сфере IT-технологий, то в 2022 г. – 522 065 подобных преступлений, что составило 26,5 % от общего количества зарегистрированных преступлений. Из этого числа в 2018 г. было выявлено 2 500 преступлений в сфере компьютерной информации (далее – компьютерных преступлений), в 2019 г. – 2 883 компьютерных преступления, в 2020 г. – 4 498 компьютерных преступлений, в 2021 г.– 6 869 компьютерных преступлений, в 2022 г. зафиксировано 10 027 преступлений данного вида. Как видим, в 2022 г. отмечается рост на 46 % в сравнении с 2021 г. При этом одним из вышеуказанных видов преступных деяний, где отмечается значительная динамика роста, выступает неправомерное воздействие на КИИ Российской Федерации, ответственность за которое предусмотрена ст. 274.1 Уголовного кодекса Российской Федерации (далее – УК РФ). В частности, если в 2018–2019 гг. преступления данного вида не регистрировались, в 2020 г. зафиксировано 22 преступления, в 2021 г. – 159 преступных деяний, то уже в 2022 г. отмечено совершение 519 деяний (рост на 226,4 % в сравнении с 2021 г.) [1].

Таким образом, повышенное значение объектов КИИ обусловлено тем фактом, что нарушение их стабильного функционирования способно стать причиной серьезных последствий. Компьютерная атака при ее правильном планировании и реализации может на 100 % остановить работу государственной КИИ, что приведет к катастрофе в общественной, экономической или финансовой сфере. В рамках противодействия противоправным деяниям подобного рода был принят Федеральный закон от 26 июля 2017 г. № 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», который дополнил УК РФ ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской

[1] О безопасности критической информационной инфраструктуры Российской Федерации: федеральный закон от 26 июля 2017 г. № 187-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.04.2023).

Федерации»[1]. Указанная статья была включена в гл. 28 раздела «Преступления против общественной безопасности и общественного правопорядка».

Постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 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"» обращает внимание судов на то, что преступления, предусмотренные статьей 274 УК РФ, признаются оконченными, когда указанные в ч. 1. ст. 274 деяния повлекли наступление одного или нескольких общественно опасных последствий в виде уничтожения, блокирования, модификации либо копирования такой информации, а также в виде причинения крупного ущерба. Кроме того, следует учитывать, что использование вредоносных компьютерных программ для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (в том числе в случае, когда осуществляется распространение этих программ на объекты критической информационной инфраструктуры исключительно для их последующего использования) полностью охватывается ч. 2 статьи 274.1 УК РФ[2].

В статье 274.1 УК РФ закреплено три самостоятельных состава преступления, являющихся специальными по отношению к составам преступлений, закрепленных в ст.ст. 272–274 УК РФ: 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 (специальный состав по отношению к преступлению, предусмотренному ст. 273 УК РФ). Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации (специальный состав по отношению к преступлению, предусмотренному ст. 272 УК РФ).

Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации (специальный состав по

[1] 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»: федеральный закон от 26 июля 2017 г. № 194-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.04.2023).

[2] Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.04.2023).

отношению к преступлению, предусмотренному ст. 274 УК РФ).

Родовым объектом рассматриваемого преступления выступает общественная безопасность, видовым объектом – общественные отношения по поводу обеспечения конфиденциальности, доступности компьютерной информации, сохранности средств, используемых для ее обработки.

Предмет преступления – компьютерная информация (ст.ст. 272, 273 УК РФ), т. е. сведения о лицах, предметах, фактах, событиях, явлениях и процессах, содержащихся в информационных системах, средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование (ст. 274 УК РФ), а также технические средства противодействия угрозам устойчивости, безопасности и целостности функционирования на территории России сети Интернет и сети связи общего пользования.

В качестве непосредственного объекта рассматриваемого деяния выступают общественные отношения, связанные с обеспечением целостного состава и сохранности компьютерных данных; в случае с рассматриваемым преступлением объект будет другим[1]. С учетом того, что функционирование объектов КИИ возможно в разнообразных отраслях, исследователи предлагают несколько подходов к определению того, что может выступать в роли объекта противоправного посягательства. Предполагается, что в качестве последнего могут выступать правоотношения, нацеленные на соблюдение безопасности КИИ как комплекса объектов повышенной государственной значимости.

В качестве предмета анализируемой преступной деятельности может рассматриваться компьютерная информация, входящая в состав КИИ, а также средства, предназначенные для ее хранения, обработки и распространения. К этому же списку относятся инфосистемы, телекоммуникационное оборудование, средства автоматизации сети и компоненты электросвязи, которые можно классифицировать как часть КИИ государства. Часть 1 ст. 274.1 УК РФ обозначает наступление уголовной ответственности за разработку, передачу, применение компьютерного программного обеспечения и других компьютерных данных, созданных специально для несанкционированного влияния на объекты КИИ[2].

Указание на заведомо противоправное назначение подобных программ и информации приводит к появлению вопроса о том, как может быть квалифицировано уже имеющееся программное обеспечение, которое предназначено для противоправного уничтожения, блокировки, изменения или копирования информации, а также принудительной остановки инструментов по защите компьютерных данных при влиянии на объекты КИИ. Законодатель не указывает на принципиальную разницу таких программ, но анализ накопленной судебной практики позволяет прийти к выводу о том, что преступники применяют вредоносное программное обеспечение, созданное не только с прямой целью нанести ущерб структуре КИИ, но и различные инструменты, разработанные для иных задач. Состав преступления по конструкции носит формальный характер, из чего следует, что преступное деяние считается совершенным с момента разработки, передачи или применения подобных программ вне зависимости от результата [2; 3].

Часть 2 ст. 274.1 УК РФ предусматривает ответственность за неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных

[1] 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»: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.04.2023).

[2] Там же.

программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации[1]. Это позволяет прийти к выводу о том, что состав преступления носит материальный характер.

Анализ судебной практики позволяет прийти к выводу о том, что данные опасения не лишены смысла. В некоторых случаях судебные органы не уделяют внимания характеру нанесенного ущерба, и в приговоре используются обобщенные формулировки. Размытая трактовка причиненного вреда позволяет отнести к противоправным действиям любое деяние, сопровождающееся или выраженное в получении неправомерного доступа к защищенным данным. Предполагается, что относительно изучаемой нормы требуется рассматривать именно причинение материального ущерба, поскольку причинение физического вреда в отношении КИИ требует квалифицировать его по другим статьям УК РФ, например, как преступления против собственности. Что касается субъективной стороны, то деяние, предусмотренное в ч. 1 ст. 274.1, может быть охарактеризовано лишь наличием прямого умысла, а преступления по ч. 2 ст. 274 могут совершаться как с прямым, так и с косвенным умыслом. В качестве субъекта рассматривается вменяемое физическое лицо, достигшее 16 лет[2].

Часть 3 ст. 2741 УК РФ устанавливает уголовную ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации. Эти правила не отражены в составе Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187; вместо этого используется понятие требований по созданию безопасных условий для значимых объектов КИИ.

Квалифицирующими признаками неправомерного воздействия на критическую информационную инфраструктуру являются совершение группой лиц по предварительному сговору или организованной группой, или лицом с использованием своего служебного положения (ч. 4 ст. 274.1 УК РФ), наступление тяжких последствий (ч. 5 ст. 274.1 УК РФ).

Как было обозначено выше, подобные результаты могут проявиться в любой отрасли, поскольку классификация объектов КИИ построена на категориях, обладающих конкретной важностью для определенной сферы деятельности[3]. Наступившие послед-

---

[1] 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»: постановление Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.04.2023).

[2] Там же.

[3] 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»: федеральный закон от 26 июля 2017 г. № 194-ФЗ // Доступ из справ.-правовой системы «КонсультантПлюс». URL: http://www.consultant.ru (дата обращения: 20.04.2023).

ствия могут носить катастрофический характер. Поскольку КИИ выступает в роли связующего элемента между целой группой секторов национальной инфраструктуры, нанесение ущерба одному звену негативно сказывается и на функциональности других направлений. Из этого следует, что тяжкие последствия могут быть выражены в критическом повреждении объектов жизнеобеспечения, оборонной отрасли, а это повлечет серьезный ущерб имущественного характера, может спровоцировать массовые смерти граждан. До дополнения ст. 274.1 УК РФ в узкоспециализированных источниках литературы указывалось на то, что деятельность преступника в случае совершения противоправного деяния в сфере компьютерных данных, направленного на нарушение безопасности КИИ, квалификация состава должна определяться по совокупности со ст. 205 УК РФ Террористический акт [4; 5].

Из вышесказанного можно сделать вывод, что ст. 274.1 УК РФ рассматривается как специальная по отношению к ст.ст. 272–274 УК РФ. Дифференциация уголовной ответственности за несанкционированные действия относительно объектов КИИ возможна в том числе в рамках вышеуказанных статей, однако законодатель выбрал другую стратегию.

СПИСОК ИСТОЧНИКОВ

1. Евдокимов К. Н. Вопросы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (по материалам судебной практики) // Российский следователь. 2023. № 5. С. 15–19.

2. Ефремова М. А. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Вестник Казанского юридического института МВД России. 2022. Т. 13. № 4 (50). С. 86–92.

3. Решетников А. Ю., Малыгин И. И. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации: вопросы квалификации // Вестник Университета прокуратуры Российской Федерации. 2021. № 2 (82). С. 111–117.

4. Монгуш Д. Р. Уголовно-правовой анализ статьи 274.1 УК РФ неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации // Законность и правопорядок в современном обществе: сборник статей по итогам Международной научно-практической конференции. 2018. С. 57–60.

5. Ларина Л. Ю. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру России // Актуальные вопросы борьбы с преступлениями. 2017. № 3. С. 22–25.

REFERENCES

1. Evdokimov K. N. Qualification issues of unlawful influence on the critical information infrastructure of the Russian Federation (based on judicial practice) // Russian investigator. 2023. No. 5. P. 15–19. (In Russ.)

2. Efremova M. A. Criminal liability for unlawful influence on the critical information infrastructure of the Russian Federation // Bulletin of Kazan Law Institute of the Ministry of Internal Affairs of Russia. 2022. Vol. 13. No. 4 (50). P. 86–92. (In Russ.)

3. Reshetnikov A. Yu., Malygin I. I. Unlawful influence on the critical information infrastructure of the Russian Federation: qualification issues // Bulletin of the University of the Prosecutor's Office of the Russian Federation. 2021. No. 2 (82). P. 111–117. (In Russ.)

4. Mongush D. R. Criminal legal analysis of Article 274.1 of the Criminal Code of the Russian Federation: unlawful influence on the critical information infrastructure of the Russian Federation // Legality and law and order in modern society: collection of articles based on the results of the International Scientific and Practical Conference. 2018. P. 57–60. (In Russ.)

5. Larina L. Yu. Criminal liability for unlawful influence on the critical information infrastructure of Russia // Current issues in the fight against crime. 2017. No. 3. P. 22–25. (In Russ.)

Информация об авторах:
А. Б. Абазов, кандидат юридических наук;
Т. А. Файрушин, без ученой степени.

Information about the authors:
A. B. Abazov, Candidate of Law;
T. A. Fayrushin, no academic degree.

Статья поступила в редакцию 25.04.2023; одобрена после рецензирования 30.08.2023; принята к публикации 17.11.2023.

The article was submitted 25.04.2023; approved after reviewing 30.08.2023; accepted for publication 17.11.2023.