УДК 349 **Юридические науки**

Дуваярова Сабина Арзу кызы, *студент,*
ФГБОУ «МГУ им Н.П. Огарёва»

ПРОБЛЕМЫ КВАЛИФИКАЦИИ НЕПРАВОМЕРНОГО ВОЗДЕЙСТВИЯ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: В данной статье рассматриваются проблемы квалификации неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации в сфере уголовного права, а также динамика применения статьи 274.1 Уголовного кодекса РФ в судебной практике.

Ключевые слова: Уголовное право, уголовные преступления, преступления в сфере компьютерной информации, неправомерное воздействие, неправомерное применение, критическая информационная инфраструктура.

Annotation: This article examines the problems of qualification of unlawful influence on the critical information infrastructure of the Russian Federation in the field of criminal law, as well as the dynamics of the application of Article 274.1 of the Criminal Code of the Russian Federation in judicial practice.

Keywords: Criminal law, criminal offenses, crimes in the field of computer information, improper influence, improper use, critical information infrastructure.

В России с каждым годом наблюдается обширное развитие сферы технологий, как и во всем мире. Техническая инфраструктура внедряется во многие сферы жизни, что обусловлено не только удобством, но и обстоятельствами настоящего времени, связанными с распространением новой короновирусной инфекции COVID-19.

Но технологические новшества используются не только обычным

населением в бытовой жизни, но также их применяют в бизнесе, в управлении организаций, во многих областях исполнительной власти, и что самое важное, в защите национальной безопасности. В частности, это касается критической информации инфраструктуры (далее – КИИ) Российской Федерации.

Нормативно правовой базой данного вопроса является Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», в нем даны определения базовым дефинициям: «критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов» [2].

Ежегодно увеличивается количество атак на критическую информационную инфраструктуру. Научно-технический центр ФГУП «ГРЧЦ» исследовал вопрос кибератак и опубликовал свои результаты. Только за первые два квартала 2021 года количество атак на КИИ увеличилось на 150% по сравнению с 2021 годом. 60% таких преступлений осуществляется другими государствами. Чаще всего преступников интересует коммерческая тайна, выход на важные объекты государства, промышленные объекты, медицинские учреждения т.д.

С целью необходимости более жесткого регулирования данного деяния и предотвращения преступления был принят Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»», вносящий изменения в УК РФ.

Статья включается в себя три формы преступного посягательства: 1) незаконный доступ, 2) создание и распространение вредоносной информации, 3) несоблюдение предписаний использования средств хранения, передачи, обработки компьютерной информации. Законодатель не стал выделять особо квалифицирующие признаки по ст. 272, 273, 274 УК РФ, а создал статью 274.1, которая в очередь является бланкетной, так как при использовании данной

статьи необходимо обращаться к Федеральному закону от 26 № 194-ФЗ [1].

Важную и проблемную часть данной нормы представляют предметы преступления, так по ч. 1 ст. 274.1 УК РФ – это компьютерная информация или компьютерные программы, которые созданы специально для осуществления кибератак, следовательно, зафиксировать и изучить данный факт возможно лишь с том случае, если установлена специальная программа защиты, предназначенная не только для защиты, но и для фиксирования программ атаки. По ч. ч. 2 и 3 ст. 274.1 УК РФ предметом являются системы различных информационных и технологический структур многих сфер.

Все значимые объекты КИИ внесены в реестр. В Приказе ФСТЭК России от 06.12.2017 N 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» закреплены сферы данных объектов: здравоохранение, наука, транспорт, связь, банковская сфера и иные сферы финансового рынка, энергетика и топливно-энергетический комплекс, атомная энергия, оборонная промышленность, ракетно-космическая промышленность, горнодобывающая промышленность, металлургическая промышленность, химическая промышленность [3].

По ч. 1 объективная сторона представляет собой три различных деяния: 1) создание, 2) использование, 3) распространение компьютерных программ или информации [4, с. 459]. Если лицо совершило все три действия, то будут квалифицировать, как единое преступление. По ч. 2 заключается в незаконном доступе к компьютерной информации. Если лицо смогло взломать системы, содержащейся в критической информационной инфраструктуре, но непредвиденным и независящим от него обстоятельствам не был причинен вред, то данное деяние будут относить к покушению по ч. 3 ст. 30, ч. 2 ст. 274.1 УК РФ.

Субъективная сторона представляет собой совершение следующих действий с прямым умыслом: создание, использование и распространение компьютерных программ или информации, созданные с целью совершения атак

[5, с. 101].

Лицо, совершая данное преступление, должно осознавать целенаправленность своих действий по отношению к структурам, представляющие собой важное значение для общества и государства.

Пробелом законодателя является не уточнение формы вины в составе нарушения правил эксплуатации средств хранения, обработки или передачи компьютерных данных, что вызывает спорные моменты при квалификации преступления.

В ч. 5 ст. 274.1 УК РФ появляется квалифицирующий признак «тяжкие последствия». Проанализировав судебную практику, стоит отметить конкретики в размере ущерба в денежном эквиваленте отсутствует. Суд самостоятельно принимает решение, то есть в зависимости от обстоятельств устанавливает тяжесть последствий.

К квалификации «тяжкие последствия» более опасные последствия, чем к «крупному ущербу», сумма ущерба которого превышает один миллион рублей. К тяжким последствиям можно отнести: разрушение и повреждение инфраструктуры, зданий, сооружений, причинение вреда национальной безопасности, гибель людей.

Практика применения данной статьи не часта, но тем не менее приговоры имеются. Так, например, первое дело по данной норме было рассмотрено в Петропавловске-Камчатском 31 мая 2019 г. Была осуществлена атака на сайты Роскомнадзора, что заблокировало доступ к сайту на 25 минут. Лицо, которое совершило преступление, было освобождено от уголовной ответственности, так как полностью признал вину и раскаялся.

Первое дело (№ 1345/ 2019), где появилось обвинение по этой статье, было рассмотрено в Петропавловске-Камчатском 31 мая 2019 г. Пострадавшие объекты КИИ – два сайта Роскомнадзора, для неправомерного воздействия на них использовалось специальное программное обеспечение, выполняющее функции нагрузочного тестирования интернет-ресурсов. Саму такую функциональность суд определил, как заведомо предназначенную для

неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для блокирования информации, содержащейся в ней. В результате доступ к сайтам был затруднен в общей сложности примерно на 25 мин. Подсудимый раскаялся и был полностью освобожден от уголовной ответственности.

По делу № 1-376/2019 было выявлено причинение имущественного вреда оборонному предприятию – субъекту КИИ. Группа из трех лиц с помощью специализированного ПО проникла через протокол RDP в компьютеры оборонного предприятия, зашифровала данные на жестком диске и потребовала выкуп, судя по сумме в рублях, в размере одного биткойна. Суд принял во внимание явку с повинной и добровольное возмещение ущерба и в особом порядке назначил наказание – по два года условного осуждения каждому из подсудимых.

В деле № 1-368/2019 от 25.09.2019 г. выявлены нарушения правил эксплуатации и предъявлены обвинения по ч. 4 ст. 274.1 УК РФ (служебное положение) работнику субъекта КИИ. Сотрудница отдела продаж компании связи в день увольнения скопировала из автоматизированной системы персональные данные абонентов и отправила по электронной почте своему знакомому. Подсудимая признала вину, судебное рассмотрение прошло в особом порядке, вынесено наказание – три года лишения свободы условно.

На основании вышесказанного, стоит сделать вывод о том, что судебная практика по ст. 274.1 не так обширно представлена, что в свою очередь, вызывает сложность ознакомления с регламентацией совершения преступных деяний, направленных на неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Библиографический список:

1. Российская Федерация. Законы. Уголовный кодекс Российской Федерации: УК: текст с изменениями и дополнениями на 8 декабря 2020 года : [принят Государственной думой 24 мая 1996 года : одобрен Советом Федерации

5 июня 1996 года]. – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/. – Режим доступа: по подписке. – Текст: электронный (Дата обращения: 05.12.2021).

2. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=220885&dst=100001#H61InqSun038EEeA1. – Режим доступа: по подписке. – Текст: электронный (Дата обращения: 05.12.2021).

3. Приказ ФСТЭК России от 06.12.2017 № 227 «Об утверждении Порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации» (Зарегистрировано в Минюсте России 08.02.2018 № 49966). – URL: https://www.consultant.ru/cons/cgi/online.cgi?req=doc&rnd=E69ED8B4A11D87B4595FE419A956A879&base=LAW&n=290538&dst=100009&field=134&stat=srcfld%3D134%26src%3D100089%26code%3D16610%26page%3Dtext%26p%3D116%26base%3DLAW%26doc%3D220885#gAzInqSUH2KEytYb2. – Режим доступа: по подписке. – Текст: электронный (Дата обращения: 05.12.2021).

4. Комментарий к Уголовному кодексу Российской Федерации (научно-практический, постатейный) / Под ред. С.В. Дьякова, Н.Г. Кадникова. 5-е изд., перераб. и доп. Москва: Юриспруденция, 2017. 1035 с. – – ISBN 978-5-9516-0695-2. – Текст: непосредственный.

5. Русскевич Е. А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий: Учебное пособие / Е. А. Русскевич. – Москва: ИНФРА-М, 2017. – 186 с. – ISBN: 978-5-16-014392-7. – Текст: непосредственный.