DOI: 10.24412/2076-1503-2025-2-128-131

ЧУРАКОВ Денис Сергеевич,
Московский государственный
юридический университет
имени О.Е. Кутафина,
магистрант,
e-mail: nk-kfea@mail.ru

ИСТОРИЧЕСКИЕ ПРЕДПОСЫЛКИ УСТАНОВЛЕНИЯ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА НЕПРАВОМЕРНОЕ ВОЗДЕЙСТВИЕ НА КРИТИЧЕСКУЮ ИНФОРМАЦИОННУЮ ИНФРАСТРУКТУРУ РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация. *В статье рассматриваются исторические предпосылки установления уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Автор анализирует процесс формирования законодательства в данной сфере, начиная с правовых норм СССР и заканчивая современным этапом цифровой трансформации. Особое внимание уделяется Федеральному закону « 187-ФЗ и статье 274.1 УК РФ, а также их роли в правоприменительной практике. Исследование основано на системном и сравнительно-правовом методах, позволяющих выявить закономерности в правовом регулировании данных правоотношений. Автор приходит к выводу о преемственности в регулировании критической информационной инфраструктуры. В работе обосновывается необходимость совершенствования уголовного законодательства для повышения защиты критической информационной инфраструктуры от преступных посягательств, основываясь на исторический опыт.*

Ключевые слова: *безопасность, информационная безопасность, информационные технологии, история, критическая информационная инфраструктура, уголовная ответственность.*

CHURAKOV Denis Sergeevich,
Moscow State Law University
named after O.E. Kutafin,
Master's student

HISTORICAL BACKGROUND OF THE ESTABLISHMENT OF CRIMINAL LIABILITY FOR UNLAWFUL IMPACT ON THE CRITICAL INFORMATION INFRASTRUCTURE OF THE RUSSIAN FEDERATION

Annotation. *The article examines the historical prerequisites for the establishment of criminal liability for unlawful impact on the critical information infrastructure of the Russian Federation. The author analyzes the process of forming legislation in this area, starting with the legal norms of the USSR and ending with the current stage of digital transformation. Special attention is paid to Federal Law 187-FZ and Article 274.1 of the Criminal Code of the Russian Federation, as well as their role in law enforcement practice. The research is based on systematic and comparative legal methods to identify patterns in the legal regulation of these legal relations..The author comes to the conclusion about continuity in the regulation of critical information infrastructure. The paper substantiates the need to improve criminal legislation to increase the protection of critical information infrastructure from criminal attacks, based on historical experience.*

Key words: *security, information security, information technology, history, critical information infrastructure, criminal liability.*

Развитие научно-технического прогресса в начале 21 века достигло такого уровня, что информационные технологии стали неотъемлемой частью жизни как рядовых обывателей, так и фактором, задающим вектор развития государства практически во всех его сферах: от экономики и международной политики, до культуры и экологии.

В Российской Федерации в последние годы выработан и реализуется комплекс мер по созданию критической информационной инфраструктуры (далее по тексту КИИ РФ) и охране указанного цифрового массива от криминальных посягательств. В числе таковых, безусловно, следует признать принятие Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также установление в 2018 году уголовной ответственности за неправомерное воздействие на данный материально-виртуальный субстрат путём введения в действующий УК РФ соответствующей нормы (ст. 274.1 УК РФ).

Вместе с тем, анализ складывающейся оперативной обстановки позволяет сделать вывод о том, что данная норма, недостаточно применяется на практике.

Однако, анализ складывающейся оперативной обстановки свидетельствует о низкой востребованности данного состава в правоприменительной деятельности. Так, например, в 2024 году (с января по сентябрь) в производстве органов предварительного расследования находилось 146 уголовных дел, возбужденных по признакам преступления, предусмотренного ст. 274.1 УК РФ. из них только 67 возбуждены в отчетном периоде, окончено производством и направлено в суд с обвинительным заключением 88 дел по которым к ответственности привлечено 33 человека [6].

Сложившаяся ситуация обусловлена рядом причин, среди которых основное место в научной литературе многочисленными исследователями (И.Р. Бегишев, И.И. Бикеев, С.Д. Гайфутдинов, Р.И. Дремлюга, К.Н. Евдокимов и др.) отводится неопределённости нормативных предписаний, закреплённых в ст. 274.1 УК РФ, снижающих эффективность её применения [1-4].

Указанные вопросы не теряют своей актуальности ввиду развития научного прогресса, оказывающего непосредственное влияние на преступность в исследуемой области в части роста профессионализма и появления новых способов совершения преступлений в сфере компьютерной информации, а также необходимости адекватного противодействия данному процессу со стороны всех заинтересованных лиц. Изложенное свидетельствуют о значимости дальнейшей разработки темы настоящей магистерской диссертации для науки и практики применения нормы, предусмотренной ст.274.1 УК РФ.

Объектом настоящей работы являются общественные отношения, складывающиеся в сфере регулирования следующих процессов: доступа к компьютерной информации; создания, использования и распространения компьютерных программ; эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

В качестве предмета исследования выступают исторические нормы законодательства, ставшие основой для современного устанавливления ответственности за преступления в сере компьютерной информации, в том числе за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст.274.1 УК РФ).

Основной **целью** работы является исследование исторических аспектов установления уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Поставленная цель предполагает решение следующих **задач:**

- исследование авторских позиций в отношении анализа исторических предпосылок установления уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации;

- изучение ранее действующего уголовного законодательства в информационной сфере.

Методологической основой работы является диалектический метод познания социально-правовых явлений, а также системный, сравнительный, структурно-функциональный и другие методы научного познания.

Криминализация любого действия или бездействия предполагает наличие определенных сложившихся условий, предваряющих развитие любого государственного образования. Вместе с тем, следует сразу же подчеркнуть, что относительно ст. 274.1 УК РФ нельзя использовать традиционный подход, применяемый различными учеными при исследовании исторических предпосылок появления указанной нормы в действующем законодательстве. Очевидно абсурдным представляется в этом смысле анализ правовых источников Древней Руси, Российской империи, государства послеоктябрьского переворота, поскольку цифровая эволюция ведет свое начало именно с 40-х г.г. XX века. Именно к этому временному периоду развитие техники, общественных отношений, а также информации в мировом измерении достигло такого состояния, при котором управлять процессом хранения, систематизации и передачи последней одной биологической особью стало практически невозможным. Это обусловило изобретение первых электронно-вычислительных материальных субстратов или ЭВМ, а в дальнейшем и появление целой науки, изучаю-

щей управление различными, в том числе информационными системами, основоположником которой принято считать американского ученого-математика Норберта Виннера[5]. Современная кибернетика апеллирует таким понятием как информационная система, состоящая из определенного числа элементов, вступающих между собой в разнообразные связи и обладающих способностью запоминания информации и взаимного обмена последней. Более подробно некоторые особенности и направления данной науки, имеющие значимость для цели настоящего исследования, будут рассмотрены нами в рамках второго параграфа настоящей главы.

В СССР широкое распространение аналоговые компьютеры получили в 1970-х г.г. XX века. Серийный выпуск позволил применять их в качестве инструментария для решения прикладных задач в различных областях науки и народного хозяйства.

Из отечественных правовых источников интерес представляет, прежде всего, уголовное законодательство СССР, в частности Уголовный кодекс РСФСР (далее по тексту УК РСФСР), принятый в 1960 году. В рамках предмета настоящего исследования следует выделить некоторые нормы, охраняющие государственные интересы, предусмотренные в Главе 1 Государственные преступления УК РСФСР. Так, например, ст. 69 УК РСФР предусматривала уголовную ответственность за вредительство. Данное деяние могло быть совершено как путем активных действий, так и бездействия. Своей целевой направленностью оно имело срыв работы государственных объектов промышленности, транспортной инфраструктуры, различных отраслей народного хозяйства, денежной системы, деятельности государственных органов или общественных организаций с целью ослабления Советского государства. В качестве средства совершения указанного криминального деяния использовались, как видно из приводимого выше текста нормы, именно ресурсы государственных или общественных предприятий, либо организаций. Можно смело утверждать, что законодатель в этом случае предполагал использование любых ресурсов, в том числе и цифровых, которые начали появляться как раз во время действия данного нормативного правового акта.

Деяние относилось к категории особо опасных государственных преступлений и наказывалось лишением свободы на срок от восьми до пятнадцати лет с конфискацией имущества.

Специальными нормами по отношению к ст. 69 УК РСФСР выступали ст.ст. 86 и 86.1 УК РСФСР. Первая предусматривала уголовную ответственность за совершенные умышленно повреждение путей сообщения и транспортных средств, средств связи или сигнализации, которое повлекло или могло повлечь крушение поезда, аварию корабля или нарушение нормальной работы транспорта и связи. Вторая включала в себя уголовно-наказуемое деяние в виде повреждения или разрушения нефте-, газопроводов и нефтепродуктопроводов, а также технологически связанных с ними объектов, сооружений, средств связи, автоматики, сигнализации, которые повлекли или могли повлечь нарушение нормальной работы трубопроводов. Оба деяния относились к иным государственным преступлениям и устанавливали реальное наказание от 3-х до 15-ти лет лишения свободы.

Логичным представляется здесь вывод о том, что дальнейшая криминализация действий, связанных с посягательствами на электронные цифровые ресурсы в отечественном законодательстве связана напрямую с процессами цифровой трансформации, которыми характеризовались основные сферы жизнедеятельности обычного человека в частности и государства в целом.

Список литературы:

[1] Бегишев И. Р., Бикеев И. И. Преступления в сфере обращения цифровой информации. Казань: Издательство «Познание», 2020. – 300 с.

[2] Гайфутдинов Р. Р. Понятие и квалификация преступлений против безопасности компьютерной информации: специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право»: Дисс. ...канд. Юрид. наук. Казань, 2017. – 243 с.

[3] Дагель П.С., Котов Д.П. Субъективная сторона преступления и ее установление. Воронеж: Издательство Воронежского университета, 1974. – 243с.

[4] Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика: Дисс. … д-ра юрид. наук: 12.00.08. М., 2021. -557 с.

[5] Норберт Виннер Кибернетика и общество. Человеческое применение человеческих существ. М.: AST publishers. 2019. С.14.

[6] Статистические данные ФГКУ «Главный информационно-аналитический центр МВД России». Форма «1- ЕГС», книга 5. Сводный отчет по России за январь-сентябрь 2024г. URL: //https://xn—b1aew.xn—p1ai/folder/101762/item/15304733/.

Spisok literatury:

[1] Begishev I. R., Bikeev I. I. Prestupleniya v sfere obrashcheniya cifrovoj informacii. Kazan': Izdatel'stvo «Poznanie», 2020. – 300 s.

[2] Gajfutdinov R. R. Ponyatie i kvalifikaciya prestuplenij protiv bezopasnosti komp'yuternoj informacii: special'nost' 12.00.08 «Ugolovnoe pravo i kriminologiya; ugolovno-ispolnitel'noe pravo»: Diss. ...kand. YUrid. nauk. Kazan', 2017. – 243 s.

[3] Dagel' P.S., Kotov D.P. Sub"ektivnaya storona prestupleniya i ee ustanovlenie. Voronezh: Izdatel'stvo Voronezhskogo universiteta, 1974. – 243 s.

[4] Evdokimov K.N. Protivodejstvie komp'yuternoj prestupnosti: teoriya, zakonodatel'stvo, praktika: Diss. … d-ra yurid. nauk: 12.00.08. M., 2021. -557 s.

[5] Nobert Vinner Kibernetika i obshchestvo. CHelovecheskoe primenenie chelovecheskih sushchestv. M.: AST publishers. 2019. C.14.

[6] Statisticheskie dannye FGKU «Glavnyj informacionno-analiticheskij centr MVD Rossii». Forma «1- EGS», kniga 5. Svodnyj otchet po Rossii za yanvar'-sentyabr' 2024g. URL: //https://xn—b1aew.xn—p1ai/folder/101762/item/15304733/.