УДК 343.3/.7

ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ерофеев Н.Г., студент гр. БЭс-211, V курс
Научный руководитель: Съедина Н.В., к.п.н., доцент
Кузбасский государственный технический университет
имени Т.Ф. Горбачева, г. Кемерово

Цифровая трансформация общественных отношений обусловила появление новых вызовов для системы уголовной юстиции. Преступность не только мигрировала в киберпространство, но и приобрела качественно новые формы, не укладывающиеся в традиционные рамки уголовно-правовых конструкций. Правоприменительная практика сталкивается с серьезными трудностями при юридической оценке деяний в сфере информационной безопасности. Данные проблемы носят комплексный характер и затрагивают как вопросы уголовно-правовой квалификации, так и процессуальные аспекты доказывания.

Статистические данные свидетельствуют о тревожной динамике. По информации Генеральной прокуратуры РФ, в 2024 году было зафиксировано более 100 тысяч преступлений в сфере компьютерной информации. При этом в суды направляются уголовные дела лишь по незначительной части из них, что свидетельствует о системных проблемах в механизме привлечения к уголовной ответственности [5].

Проблемы квалификации преступлений в данной сфере традиционно начинаются с определения объекта преступного посягательства. Сложность заключается в том, что компьютерные технологии могут выступать в различных качествах: как предмет преступления, как средство совершения деяния или как среда совершения преступления. В правоприменительной практике нередки ситуации, когда одно и то же деяние может быть квалифицировано по разным статьям Уголовного кодекса в зависимости от того, как правоприменитель определит основной объект посягательства.

Одной из наиболее сложных проблем квалификации является разграничение собственно компьютерных преступлений (глава 28 УК РФ) и традиционных преступлений, совершенных с использованием информационных технологий. В первом случае компьютерная информация выступает непосредственным предметом посягательства, во втором – компьютер является лишь инструментом совершения преступления. Например, при неправомерном доступе к базе данных кадастровой палаты с целью копирования персональных данных возникает вопрос о правильности квалификации по ст. 272 УК РФ либо о необходимости применения норм о разглашении тайны. В связи с этим принципиальное значение для корректной квалификации имеет четкое отграничение информации, составляющей охраняемую законом тайну, от информации, защищаемой собственником [1, 4].

Квалификация преступлений неразрывно связана с доказыванием наличия состава преступления. В сфере информационной безопасности доказательственный аспект приобретает особую сложность. Классические критерии допустимости доказательств (надлежащий субъект, источник и способ получения), сформированные в эпоху «бумажного» делопроизводства, сталкиваются с новыми вызовами при оценке цифровых данных. Ключевой проблемой выступает обеспечение надлежащей цепочки хранения цифровых доказательств (chain of custody). В судебной практике нередки случаи, когда доказательства признаются недопустимыми из-за сомнений в их аутентичности или нарушений порядка получения. Хотя в УПК РФ появилась категория «электронные носители информации», правоприменительная практика выявляет недостаточную регламентацию порядка их изъятия и исследования [2].

Глобальный характер сети Интернет обусловливает трансграничность большинства киберпреступлений. Преступник может находиться на территории одного государства, жертва – на территории другого, а серверы с доказательствами – на территории третьего. Это порождает сложнейшие вопросы определения места совершения преступления и применимого уголовного закона. Значимым событием в развитии международного сотрудничества стало принятие в 2024 году Конвенции ООН против киберпреступности, которая способствует единообразию в части правового статуса электронных доказательств и виртуальных активов. Однако ряд важных вопросов, таких как узость перечня уголовных правонарушений и устаревшие юрисдикционные привязки, не нашел отражения в итоговой версии документа [3].

Активное внедрение технологий искусственного интеллекта создает ситуации, когда традиционные субъектные конструкции уголовного права оказываются неприменимыми. Вопрос о том, является ли программа на основе ИИ орудием преступления или «соучастником», пока не находит однозначного ответа ни в доктрине, ни в практике. Законодатель предпринимает определенные шаги: планируется усилить наказание за применение искусственного интеллекта при совершении мошеннических киберпреступлений, а также признать цифровую валюту имуществом для целей УК РФ, что позволит накладывать на нее арест.

Исходя из вышеперечисленного, можно предложить ряд мер, направленных на повышение эффективности квалификации преступлений в сфере информационной безопасности.

Во-первых, необходимо совершенствование законодательной техники. Требуется уточнение понятийного аппарата, закрепление в законе определений новых видов киберпреступлений и установление четких критериев разграничения смежных составов. Важным направлением выступает приведение бланкетного законодательства в соответствие с уголовно-правовыми нормами.

Во-вторых, учитывая техническую сложность рассматриваемых дел, необходима специализация правоприменителей. Мировой опыт демонстрирует эффективность создания специализированных подразделений по

расследованию киберпреступлений и специализированных судебных составов, что могло бы повысить качество рассмотрения соответствующих категорий дел.

В-третьих, требуется создание эффективной системы экспертного обеспечения. Целесообразно формирование специализированных судебно-экспертных учреждений в области компьютерно-технической экспертизы, а также введение института специалистов в уголовный процесс по делам рассматриваемой категории.

В-четвертых, необходимо совершенствование процессуального законодательства в части регламентации порядка собирания и оценки электронных доказательств. Требуется разработка четких критериев их допустимости, учитывающих специфическую природу цифровых данных.

Таким образом, проблемы квалификации преступлений в сфере информационной безопасности носят комплексный характер и обусловлены как стремительным развитием технологий, так и несовершенством законодательной техники. Статистика демонстрирует критически низкий процент уголовных дел, направляемых в суд, что свидетельствует о системных проблемах в расследовании данных преступлений. Решение обозначенных проблем требует системного подхода, включающего совершенствование законодательства, развитие системы экспертного обеспечения и активизацию международного сотрудничества. Только комплексное решение указанных проблем позволит обеспечить неотвратимость ответственности за киберпреступления в условиях цифровой трансформации общества.

Список литературы:

1. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (в действ. ред.) // [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891

2. Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 № 174-ФЗ (в действ. ред.) // [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102073942

3. Конвенция Организации Объединенных Наций против киберпреступности (Заключена в г. Нью-Йорке 24.12.2024) // [Электронный ресурс] URL: https://www.un.org/ru/documents/treaty/A-RES-79-243

4. ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (в действ. ред.) // [Электронный ресурс] URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264

5. Состояние преступности в Российской Федерации // Официальный сайт Генеральной прокуратуры РФ // [Электронный ресурс]. – Режим доступа: https://genproc.gov.ru/stat/data/