УДК 343.2

Савин Кирилл Сергеевич
Студент 2 курса магистратуры,
Институт технологий предпринимательства и права
Санкт-Петербургский государственный университет аэрокосмического приборостроения
Россия, г. Санкт-Петербург

ОТВЕТСТВЕННОСТЬ ЗА СОВЕРШЕНИЕ ПРЕСТУПЛЕНИЙ В ИНФОРМАЦИОННОЙ СФЕРЕ: АНАЛИЗ И ПРОБЛЕМЫ КВАЛИФИКАЦИИ

Аннотация: *В статье проведен анализ главы 28 УК РФ, посвященной преступлениям в сфере компьютерной информации, рассмотрены проблемы, возникающие при их квалификации, и сформулированы предложения по совершенствованию действующего уголовного законодательства в области информационной безопасности.*

Ключевые слова: *уголовная ответственность, преступления в информационной сфере, квалификация, вредоносная программа, неправомерный доступ к компьютерной информации, состав преступления.*

RESPONSIBILITY FOR COMMITTING CRIMES IN THE INFORMATION SPHERE: ANALYSIS AND PROBLEMS OF QUALIFICATION

Summary: *The article analyzes Chapter 28 of the Criminal Code of the Russian Federation devoted to crimes in the field of computer information, considers the problems arising during their qualification, and formulates proposals for improving the current criminal legislation in the field of information security.*

Keywords: *criminal liability, crimes in the information sphere, qualification, malware, unauthorized access to computer information, the composition of the crime.*

Согласно аналитическому отчету МВД, с января по ноябрь 2022 года в России зафиксировано 470,1 тыс. преступлений в сфере компьютерных технологий и информационной безопасности [1]. Несмотря на легкое снижение на 4,9% по сравнению с предыдущим годом и уменьшение удельного веса этих преступлений на 1,6%, они по-прежнему представляют серьезную опасность для общества.

В законодательстве РФ предусмотрена ответственность за преступления в области компьютерной информации в соответствии с гл. 28 УК РФ, которая включает в себя несколько статей: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных компьютерных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» и ст. 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования»[2].

Статистические данные указывают на уменьшение количества преступлений в информационной сфере, но из-за высокой латентности таких преступлений, реальное число может быть значительно выше числа, отраженного в статистических данных. Это обусловлено спецификой преступных деяний и необходимостью разработки специальных методов

раскрытия преступлений в информационной сфере, а также тем, что потерпевшие часто не желают обращаться в правоохранительные органы, предпочитая другие способы защиты своих прав. Также, существуют проблемы с квалификацией преступлений в информационной сфере.

В Российской Федерации ст. 272 УК РФ предусмотрена уголовная ответственность за «неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожений, блокирование, модификацию либо копирование компьютерной информации». Законодательство определяет компьютерную информацию как «сведения (сообщения, данные), представляемые в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [2]. Однако термин «охраняемая законом компьютерная информация» не имеет четкого определения, что создает проблемы при применении ст. 272 УК РФ. Существует мнение, что статья не применима к неправомерным действиям с открытой информацией. Тем не менее, судебная практика показывает, что статья может применяться и к общедоступной информации. Суды, как правило, ссылаются на Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [3], который определяет понятие «защита информации» как правовые, организационные и технические меры, направленные на «обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации» [4].

Согласно ст. 273 УК РФ, незаконное «создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной

информации или нейтрализации средств защиты компьютерной информации», влечет уголовную ответственность. Преступления, связанные с использованием вредоносных программ, являются распространенными и представляют серьезную угрозу для информационной безопасности. Вредоносные программы, упоминаемые в ст. 273 УК РФ, могут включать в себя различные виды вирусов, троянов, червей, руткитов, фишинговые атаки, кейлоггеры и спам [5]. Важно отметить, что в научном правовом сообществе нет единого понимания, что именно является вредоносной программой.

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения», вредоносной программой является программа, разработанная для несанкционированного доступа к информации и/или воздействия на информацию или ресурсы информационной системы [6]. Однако существует множество программ, созданных с целью или способствующих выполнению несанкционированных действий в информационной системе, которые не подпадают под это определение. Например, вирусы, которые собирают данные о пользователях устройств без их ведома, не нанося при этом непосредственного вреда операционной системе. Это указывает на необходимость более широкого толкования понятия вредоносной программы в правовой науке и законодательстве.

Ст. 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, а также правил доступа к информационно-телекоммуникационным сетям, что привело к уничтожению, блокированию, модификации или копированию компьютерной информации и причинило крупный ущерб. Однако, как правило, нет четких и однозначных норм эксплуатации оборудования и обработки информации, а также строгого перечня правил доступа к информационным сетям. Поэтому, в данном случае, ответственность должна быть закреплена за правомочным лицом, которое должно обеспечивать безопасную эксплуатацию и доступ к информационно-

телекоммуникационным сетям, а также регулярно обновлять правила и нормы для предотвращения возможных нарушений. Это позволит минимизировать риски возникновения ситуаций, когда нормы и правила неопределенны или неясны, а также снизить возможность крупных ущербов для охраняемой компьютерной информации.

Ст. 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» отсылает нас к Федеральному закону от 26 июля 2017 г. № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации» [7]. Особенностью предмета преступления является то, что в качестве такового выступают программы, предназначенные для совершения компьютерных атак на объекты критической информационной инфраструктуры.

Стоит заметить, что существует множество преступлений, связанных с использованием информационной среды, которые не ограничиваются теми, что предусмотрены вышеупомянутыми статьями. В частности, мошенничество в сфере информационных технологий является распространенным видом преступлений, и по мере развития информационной среды появляются новые способы его совершения. В качестве объектов мошеннических преступлений в информационной сфере часто выступают мобильные и компьютерные программы, социальные сети, онлайн-платежи и интернет-банкинг, электронные кошельки и облачные хранилища данных.

В мире информационных технологий киберпреступники постоянно совершают новые виды преступлений, и использование вредоносных программ с целью хищения денежных средств – один из наиболее распространенных. Хакеры используют все более изощренные методы, чтобы получить доступ к банковским счетам, электронным кошелькам и другим ресурсам, на которых хранятся ценные данные. Поводами для возбуждения уголовных дел становятся заявления граждан и юридических лиц, а оперативно-розыскные мероприятия специализированных подразделений

МВД и ФСБ помогают выявлять преступников и пресекать их действия. Ст. 273 УК РФ призвана обеспечить защиту граждан и бизнеса от киберпреступлений и наказать тех, кто злоупотребляет информационными технологиями для своих личных выгод.

Современные технологии не только улучшают нашу жизнь, но и создают новые возможности для преступников. Появление новых форм мошенничества и изменение способов их совершения требуют обновления законодательства, в том числе и уголовного кодекса. Очевидна необходимость расширения перечня электронных преступлений и уточнения определения некоторых из них, так как в настоящее время не все способы нарушения безопасности компьютерной информации подпадают под законодательство. Одним из ключевых вопросов является определение перечня компьютерных преступлений. Необходимо внести изменения в УК РФ, чтобы охватить новые формы преступлений, совершаемых в электронной среде, включив в определение преступления понятие «с применением компьютерных средств» или «в сфере компьютерной информации». Также необходимо уточнить дополнительные признаки в ст. 272 УК РФ, которые предусматривали бы различные способы получения доступа к компьютерной информации, поскольку существующее понятие «неправомерный доступ» не отражает всех способов нарушения правил доступа к информации.

Таким образом, существующее законодательство, регулирующее сферу информационных технологий и киберпреступности, нуждается в доработке и совершенствовании. Несмотря на широкое распространение и высокую опасность для общества, связанную с данными видами преступлений, законодательство не всегда предоставляет ясное и однозначное толкование многих понятий. Кроме того, расследование киберпреступлений является сложным процессом, и это дополнительно подчеркивает необходимость обновления уголовного законодательства в данной области. Одним из наиболее актуальных направлений усовершенствования законодательства

является восполнение имеющихся пробелов в 28 главе УК РФ, которая касается компьютерных преступлений.

Использованные источники:

1. Состояние преступности в России // Министерство внутренних дел Российской Федерации ФКУ «Главный информационно-аналитический центр». – [Электронный ресурс]. – Режим доступа: https://d-russia.ru/wp-content/uploads/2022/12/mvd_22_11_.pdf (дата обращения 13.02.2023).
2. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ (с посл. изм. и доп. от 29 декабря 2022 г. № 586-ФЗ) // Официальный интернет-портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 17.02.2023).
3. Русскевич Е.А. Неправомерный доступ к компьютерной информации: теория и судебная практика // Судья. – 2018. – № 10 (94). – С. 46-50.
4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с посл. изм. и доп. от 29 декабря 2022 г. № 604-ФЗ) // Официальный интернет–портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 17.02.2023).
5. Александров Л.П. Предупреждение и раскрытие оперативными подразделениями внутренних дел фактов мошенничества в сфере информационных технологий. Материалы XXIV Международной студенческой научной конференции «Молодежь, наука и цивилизация». – Красноярск: СибЮИ МВД России, 2022. – С. 365-368.
6. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – [Электронный ресурс]. – Режим доступа: http://docs.cntd.ru/document/1200058320 (дата обращения: 17.02.2023).

7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической инфраструктуры Российской Федерации» // Официальный интернет–портал правовой информации. – [Электронный ресурс]. – Режим доступа: http://www.pravo.gov.ru/ (дата обращения: 17.02.2023).