УДК 349 **Юридические науки**

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

ПРАВОВОЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА РОССИИ В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ПРЕСТУПЛЕНИЯМ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Аннотация: В данной статье рассматриваются преступления с использованием современных технологий сфере компьютерной информации. Проводится анализ статей Уголовного кодекса РФ, регулирующие указанное направление, а также примеры из судебной практики.

Ключевые слова: Компьютерная информация, цифровая информация, цифровые преступления, компьютерные преступления.

Annotation: This article discusses crimes using modern technologies in the field of computer information. The analysis of articles of the norms of the Criminal Code of the Russian Federation regulating this direction, as well as examples from judicial practice, is given.

Keywords: Computer information, digital information, digital crimes, computer crimes.

В настоящее время в современном обществе большое развитие получают информационные технологии, а, следовательно, расширяется распространение преступлений в сфере компьютерной информации. Как в теории, так и в практике не имеется общего понятия данной категории преступлений. В общем смысле под преступлением с использованием информационных технологий понимают общественно-опасные деяния, нарушающие уголовное законодательство и совершающиеся с целью хранения, обработки и передачи компьютерной информации [4, с. 510].

Общая цифровизация населения создает условия для разработки и закрепления необходимой государственной политики и нормативно-правовых актов. В 2017 году Президентом Российской Федерации была утверждена разработанная Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы.

В Стратегии отражены цели, задачи и меры по реализации внутренней и внешней политики Российской Федерации в сфере применения информационных и коммуникационных технологий, направленные на развитие информационного общества, формирование национальной цифровой экономики, обеспечение национальных интересов и реализацию стратегических национальных приоритетов. В целях реализации данной Стратегии была разработана и утверждена программа «Цифровая экономика Российской Федерации» [2].

Изучая состав преступлений в сфере компьютерной информации Л. Е. Шведова и В. А. Номоконов отметили, что компьютер – это объект или орудие, с помощью которых осуществляется умышленное преступление. Уголовная доктрина включает в себя ряд направлений: понятие, значение, методы, состав цифровых преступлений [6, с. 50]. Гребеньков А. А. заметил, что система противоправных деяний, совершенных при помощи компьютерно-информационных технологий и средств, где объект преступных посягательств – это компьютерная информация [3, с. 136.] В Уголовном кодексе Российской Федерации закреплена 28 глава «Преступления в сфере компьютерной информации», в которой содержатся статьи, регулирующие указанные преступные деяния в судопроизводстве.

Стоит более детально и подробно проанализировать нормы, закрепленные в главе двадцать восемь Уголовного кодекса РФ.

Стоит начать с неправомерного доступа к компьютерной информации (ст. 272 УК РФ). Объектом данного преступления являются общественные отношения, создающие и сохраняющие правомерный доступ, а также создание, хранение компьютерной информации. Предметом выступает непосредственно

компьютерная информация. И в соответствии с примечанием 1 к анализируемой статье под компьютерной информацией понимаются сведения в форме технологических сигналов (вне зависимости от средств их хранения, обработки и передачи).

Объективная сторона неправомерного доступа к компьютерной информации – действие, которое состоит в неправомерном доступе к охраняемой законом компьютерной информации. Для признания доступа неправомерным необходимо, чтобы информация была определенным образом защищена собственником, т.е. не находилась в общем доступе. Данный вывод следует из анализа положений п. 4 ст. 16 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно которому обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить помимо прочего предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации.

Субъект преступления вменяемое лицо с шестнадцати лет. Квалифицированный состав преступления (ч. 3 ст. 272 УК РФ) предусматривает уголовную ответственность за действия, совершенные специальным субъектом – лицом с использованием своего служебного положения. Субъективная сторона рассматриваемого преступления характеризуется умышленной формой вины.

Квалифицирующими признаками рассматриваемого состава преступления являются: причинение крупного ущерба (согласно примечанию 2 к ст. 272 УК РФ – ущерб, сумма которого превышает один миллион рублей), совершение деяния из корыстной заинтересованности (ч. 2 ст. 272 УК РФ); совершение деяния группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения (ч. 3 ст. 272 УК РФ); совершение деяния, если оно повлекло тяжкие последствия или создало угрозу их наступления (ч. 4 ст. 272 УК РФ).

До 2011 существовала редакция квалифицированного состава

неправомерного доступа к компьютерной информации ст. 272 УК, которая представлялась недостаточно проработанной в части такого признака как совершение деяния лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети. К числу специальных субъектов относили отдельных должностных лиц, программистов, операторов ЭВМ, наладчиков оборудования, специалистов-пользователей автоматизированных рабочих мест и т.д. В связи с чем вызывало вопросы отнесение слов «те же действия» – т.е. неправомерный доступ – к лицам, имеющим доступ к ЭВМ, системе, сети, так как они используют и рассматривают компьютерную информацию, чаще всего, правомерно. Неудачным также являлось применение в тексте статьи термина ЭВМ, который чаще всего интерпретируется, как синоним компьютера, что в действительности не одно и то же. Данные дилеммы были учтены, и в 2011 году был принят Федеральный закон № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». С помощью данного нормативно-правового акта было введено понятие об «охраняемой законом компьютерной информации», которая включает в себя не только информацию, которую наделили признаками конфиденциальности, но и любая информация, в отношении которой установлен любой правовой режим, т. е., если она признана объектом правоотношения. Законодатель целенаправленно сузил предмет преступления ст. 272 Уголовного кодекса РФ, что повлекло снижению уровня защиты, данной категории преступлений [5, с. 28].

Что касается ст. 273 УК РФ, то в ней отражена ответственность за создание, использование и распространение вредоносных компьютерных программ. Указанное преступление наносит вред средствам защиты компьютерной информации и в нормативно-правовых актах отмечено, что наносящий вред программы целенаправленные аккумулировать и уничтожить защиту компьютерной информации [2, с. 24]. Примером из судебной практики служит следующее судебное решение № 1-170/2017: в г. о. Тольятти Тюгаев Б.А. незаконно приобрел программное обеспечение, использовал и распространял вредоносные компьютерных программ, то есть заведомо предназначенных для

несанкционированной нейтрализации средств защиты компьютерной информации, совершенные из корыстной заинтересованности при следующих обстоятельствах. которое состоит из библиотек и приложений, и контрафактное программное обеспечение обозначив денежное вознаграждение за свои услуги в сумме 600 рублей. Ему назначили наказание: по ст. 146 ч. 3 п. «в» УК РФ в виде одного года двух месяцев лишения свободы, по ст. 273 ч. 2 УК РФ в виде одного года лишения свободы. Проблематикой данной нормы является то, что отсутствует закрепленный перечень программ, которые относятся к вредоносным. Поэтому возникают сложности при определении того, относить ли, используемую при совершении преступления программу к разряду вредоносных или нет. Бердник М.В. считает, что данное обстоятельство является пробелом в законодательстве. Но, нельзя оставить без внимания тот факт, что такие программы обновляются, переименовываются, совершенствуются очень стремительно и быстро, что и вызывает сложности для создания перечня таких программ.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. 274 статья УК РФ является бланкетной, так как инструкции средств хранения либо же обработки, передачи технологической информации. Можно разделить правила эксплуатации на нормативно-правовые и индивидуальные акты. Индивидуальные акты, например, регламенты по эксплуатации компьютеров, разработанные собственником компьютерного оборудования, являются распоряжениями индивидуального характера, обращенными к определенному кругу лиц и обязательными для исполнения только этими лицами. Можно сделать вывод, что нельзя привлекать к уголовной ответственности по ст. 274 УК РФ лиц, не исполнивших предписания, установленных индивидуальными актами (техническая документация производителя и т.п.), если это не связано с разглашением или передачей конфиденциальной информации. Мы считаем, что законодатель под анализируемыми правилами понимает не любые положения инструкций и иных

предписаний собственника или владельца компьютерного оборудования и компьютерной информации, а только те, которые имеют нормативный и обязательный характер.

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. 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. Из неширокого перечня судебной практики по данной норме, которые имеются на официальных сайтах судов, в большинстве случаев подсудимый признает вину и раскаивается, что приводит к судебному рассмотрению в особом порядке. То есть отсутствует противоположное мнение подсудимого к обвинению, и не предоставляется возможным изучения тактики защиты. Только в средствах массовой информации (газетах, журналах и т.д.) можно найти освещенные уголовные дела по данной норме с обвинительным приговором, где детали и факты разбирательства могут быть искажены или интерпретированы неверно.

Подводя итог, стоит отметить, что российское законодательство включает в себя широкий сектор для регулирования и предотвращения уголовных компьютерно-информационных преступных деяний, но нормативную базу следует обновлять, расширять и совершенствовать, чтобы соответствовать изменяющимся информационным технологиям и усложняющимся преступлениям данной категории.

Библиографический список:

1. Российская Федерация. Законы. Уголовный кодекс Российской Федерации: УК: текст с изменениями и дополнениями на 1 июля 2021 года:

[принят Государственной думой 24 мая 1996 года : одобрен Советом Феде-рации 5 июня 1996 года]. – Текст: электронный – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst978 (дата обращения: 04.07.2022).

1. Распоряжение Правительства РФ от 28.07.2017 № 1632-р «Об утверждении программы «Цифровая экономика Российской Федерации». – Текст: электронный – URL: http://www.consultant.ru/document/cons_doc_LAW_221756/ (дата обращения: 05.07.2022).

2. Бегишев И. Р. Информационное оружие как средство совершения преступлений / И. Р. Бегишев. – Текст: непосредственный // Информационное право. – 2010. – № 4. – С. 23–25. – URL: https://wiselawyer.ru/poleznoe/43677-informacionnoe-oruzhie-sredstvo-sovershenija-prestuplenij (дата обращения: 05.07.2022).

3. Гребеньков А. А. Общие подходы к определению понятия «компьютерная информация» в уголовно-правовой теории / А. А. Гребеньков. – Текст: непосредственный // Известия Юго-Западного государственного университета. Серия: История и право. – 2012. – № 1-2. – С. 135–138. – URL: https://elibrary.ru/item.asp?id=20214036 (дата обращения: 05.07.2022).

5. Кучина Я. О. Понятие компьютерной информации и его влияние на квалификацию преступлений, предусмотренных статьей 272 Уголовного кодекса Российской / Я. О. Кучина. – Текст: непосредственный // Академический юридический журнал. – 2019. – № 2 (76). – С. 25-34. – URL: https://www.researchgate.net/publication/335617367_PONATIE_KOMPUTERNOJ_INFORMACII_I_EGO_VLIANIE_NA_KVALIFIKACIU_PRESTUPLENIJ_PREDUSMOTRENNYH_STATEJ_272_UGOLOVNOGO_KODEKSA_ROSSIJSKOJ_FEDERACII (дата обращения: 05.07.2022).

6. Номоконов В. А., Тропина Т. Л. Киберпреступность как новая криминальная угроза / В. А. Номоконов, Т. Л. Тропина. – Текст: непосредственный // Криминология: вчера, сегодня, завтра. – 2012. – № 24. – С.

45–55. – URL: https://cyberleninka.ru/article/n/kiberprestupnost-kak-novaya-kriminalnaya-ugroza (дата обращения: 05.07.2022).

7. Интернет-портал «Судебные и нормативные акты РФ». – Текст: электронный – URL: https://sudact.ru/ (дата обращения: 03.07.2022).