УДК 343.3/.7 **Юридические науки**

Кшнякина Анастасия Евгеньевна, *студентка юридического факультета, специальность «Правоохранительная деятельность» МГУ им. Н.П. Огарева, Россия, Саранск*

Петрикова Светлана Васильевна, *научный руководитель, кандидат юридических наук, доцент кафедры уголовного права, криминалистики, криминологии юридического факультета МГУ им. Н.П. Огарева*

АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ СТ.273 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ

Аннотация: в статье раскрывается понятие преступлений в сфере компьютерной информации, определяется понятие вредоносных компьютерных программ, выделяются актуальные проблемы применения ст. 273 Уголовного кодекса РФ, предлагаются пути их разрешения.

Ключевые слова: вредоносные программы, использование, компьютерная информация, распространение, создание.

Annotation: the article reveals the concept of crimes in the field of computer information, defines the concept of malicious computer programs, highlights the actual problems of applying Article 273 of the Criminal Code of the Russian Federation, suggests ways to resolve them.

Key words: crime, computer information, malware, judicial practice.

В условиях развития информатизации, электронных и цифровых технологий особо актуализируется вопрос о защите прав человека в информационном пространстве, в сети Интернет. Граждане РФ, имея доступ и пользуясь возможностями интернета, должны быть уверены в защите своих прав государством, но также должны соблюдать законы, которые регулируют эти

права, только тогда каждый будет уверен, что его права, данные Конституцией не будут нарушены в современном информационном мире [2, с. 15].

Глава 28 Уголовного кодекса Российской Федерации содержит составы, предусматривающие ответственность за преступления в сфере компьютерной информации. По мнению А. И. Чучаева преступлениями в сфере компьютерной информации являются общественно опасные деяния, которые причиняют вред или создают опасность причинения вреда безопасности создания, хранения, использования либо распространения информации или информационных ресурсов, закрепленные в уголовно-правовом законодательстве [3, с. 156]. В статье мы подробнее рассмотрим ст. 273 Уголовного кодекса (создание, использование и распространение вредоносных компьютерных программ). Речь в данной статье идет об охране и защите компьютерных программ от вредоносного воздействия на них с помощью компьютерных вирусов и запрещенных программ. В законе не закреплено понятие «вредоносные компьютерные программы», но чаще всего такими признают компьютерные программы или переносные коды, которые направлены на хищение информации и подрыва функциональности программного обеспечения. Ими могут являться компьютерные вирусы, черви, программы-сканеры, эмуляторы электронных средств защиты, программы управления потоками компьютерной информации и т.д.

Маслакова Е.А. обозначает вредоносную программу как компьютерную программу, функционирование которой вызывает не санкционированное собственником компьютерной информации ее уничтожение, блокирование, модификацию либо копирование [5, с. 70]. Иную компьютерную информацию в примечании 1 статьи 272 Уголовный кодекс определяет, как сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [1].

Объективная сторона данного состава преступления заключается в трех формах деяния: создании, распространении или использовании компьютерных программ либо иной компьютерной информации, которые заведомо, на

начальном этапе направлены на уничтожение, блокирование, модификацию, ко пирование компьютерной информации или нейтрализации средств защиты компьютерной информации. Следует остановиться на данном элементе состава преступления, так как исходя из буквального толкования диспозиции нормы следует, что ответственность наступает с момента создания вредоносных программ, которая включает в себя результат деятельности, выразившийся в выполнении команд, предназначенных для подрыва нормального функционирования информационно-телекоммуникационных сетей, компьютерных устройств, с целью уничтожения, блокирования, модификации, копирования компьютерной информации.

Макушев Д. И. в своей статье указывает, что даже поверхностный взгляд на диспозицию ст. 273 УК РФ позволяет сделать вывод об отсутствии наказания за приобретение преступниками вредоносного программного обеспечения. Приобретение таких программ рассматривается как приготовление к преступлению путем приискания лицами орудий или средств совершения будущего преступления [4, с. 612]. Изучая судебную практику по делам о создании, распространении и использовании вредоносных компьютерных программ следует указать на то, что в описательно-мотивировочной части приговора указывается момент приобретения вирусных программ и изучения соответствующей литературы, но по факту на квалификацию данные действия не влияют. Преступление считается оконченным с момента совершения хотя бы одного из альтернативных действий, указанных в статье, то есть о приобретении программ речи не идет.

Следует выделить проблему квалификации преступлений по данной статье, связанную с объективно повышенной латентностью и сложной спецификой выявления и предупреждения преступлений сотрудниками правоохранительных органов. В связи с этим практика движется к уменьшению количества раскрытых и доведенных до судебного разбирательства дел о преступлениях, предусмотренных статьей 273 УК РФ.

Все чаще в практике встречается квалификация DDoS-атак по изученной статье. DDoS-атака (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании») – это хакерская атака, выполняемая одновременно с большого числа устройств на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён [8].

Так, согласно приговору № 1-129/2019 от 8 августа 2019 г. по делу № 1-129/2019, Беспамятнов М.Р., 14.03.2018 г., находясь по адресу своего места жительства, использовал вредоносную компьютерную программу (типа DDoS), совершив несанкционированные сетевые воздействия в виде компьютерных атак на Интернет – ресурс Центральной избирательной комиссии Российской Федерации с электронным адресом «www.cikrf.ru», с целью неправомерного блокирования компьютерной информации, размещенной на указанном ресурсе [6].

Продолжая реализовывать свой преступный умысел, Беспамятнов М.Р. 14.03.2018 г., с целью проверки практических навыков использования вредоносных компьютерных программ, использовал вредоносную компьютерную программу, совершив несанкционированные сетевые воздействия в виде компьютерных DDoS-атак на Интернет – ресурс администрации городского поселения-город Павловск Павловского муниципального района Воронежской области с электронным адресом «www.pavlovskadmin.ru».

Действия подсудимого суд квалифицировал по ч. 1 ст. 273 УК РФ как использование компьютерной программы, заведомо предназначенной для несанкционированного блокирования компьютерной информации.

В другом случае по делу № 1-14/2014 было установлено, что 27 сентября 2012 года в ночное время, более точное время следствием не установлено, действуя умышленно, незаконно, из корыстных побуждений, за денежное вознаграждение, в целях несанкционированного блокирования доступа

легальных пользователей сети Интернет к информации, содержавшейся на Интернет-ресурсе, принадлежащим «Ф.К.», Монид Ю. С. отправил команду на начало DDoS-атаки, указанные выше вредоносные программы, действуя скрытно для пользователей компьютеров, входивших в состав каждой ботнет-сети, инициировали аномально большое количество TCP-соединений (SYN-Flood), отправку аномально большого количества HTTP Get запросов, а также отправку аномально большого количества сетевых пакетов по протоколам UDP и ICMP на Интернет-ресурс принадлежащий «Ф.К.» что привело к блокированию информации, размещенной на указанном Интернет-ресурсе, для доступа легальных пользователей сети Интернет.

Суд квалифицировал действия Монид Ю.С. по ч. 2 ст. 273 УК РФ.

Как следует из выше представленной судебной практики, действия подсудимых были квалифицированы по статье 273 УК РФ.

Таким образом, по нашему мнению, правоохранительным органам необходимо повышать уровень расследования преступлений в сфере компьютерной информации, в связи с их латентностью необходимо также разрабатывать соответствующие новые методики, применяемые для раскрытия преступлений, а законодателю необходимо закрепить в диспозиции статьи такое деяние объективной стороны преступления, как приобретение вредоносного программного обеспечения и иной компьютерной информации.

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 Федерации 5 июня 1996 года]. – Текст: электронный – URL: http://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/#dst978 (дата обращения: 02.07.2022).

2. Васильцова, Е. В. Значение защиты прав человека в информационном пространстве / Е. В. Васильцова. – Текст: непосредственный // Новый

юридический вестник. – 2019. – № 5 (12). – С. 12-15. – URL: https://moluch.ru/th/9/archive/137/4371/ (дата обращения: 02.07.2022).

3. Грачева Ю. В., Маликов С. В., Чучаев А. И. Преступления в сфере компьютерной информации: критический взгляд // Право. – Журнал Высшей школы экономики. – 2021. – № 4. – С. 152-176.

4. Макушев, Д. И. О совершенствовании объективной стороны состава преступления, предусмотренного ст. 273 УК РФ / Д. И. Макушев. – Текст: непосредственный // Молодой ученый. – 2016. – № 6 (110). – С. 611-613. – URL: https://moluch.ru/archive/110/26922/ (дата обращения: 02.07.2022).

5. Маслакова Е. А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: дис. ... канд. юрид. наук. – М., 2008. – 198 с.

6. Интернет-портал «Судебные и нормативные акты РФ». – Текст: электронный – URL: https://sudact.ru/ (дата обращения: 02.07.2022).

7. Рарог А. И. Постатейный комментарий к Уголовному кодексу РФ / А. И. Рарог. – Москва: Эксмо, 2019. – 720 с. – ISBN 978-5-04-108395-3. – Текст: непосредственный.

8. Peng Liu. Denial of Service Attacks. – University Park. – 2004. – Текст: электронный – URL: https://ru.wikipedia.org/wiki/DoS-атака#cite_note-_008c862591ba87b1-1 (дата обращения: 02.07.2022).