ОТГРАНИЧЕНИЕ МОШЕННИЧЕСТВА В СЕТИ ИНТЕРНЕТ ОТ СМЕЖНЫХ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Яковлева Я.Ю.

Научный руководитель: Инюшкин А.А.

Россия, г. Самара,
Самарский национальный исследовательский университет
имени академика С.П. Королева

Аннотация. *В статье рассмотрены преступления в сети Интернет и в сфере компьютерной информации. Приведены различия между составами преступлений. Выделены особенности каждой из статей данных преступлений. Приведена статистика по ст. 159.6, 272, 273, 274 и 274.1.*

Ключевые слова: *мошенничество в сети Интернет, преступления в сфере компьютерной информации, разграничение преступлений, компьютерная информация.*

Последние несколько десятилетий значительно увеличили доступность электронных ресурсов. Благодаря этому появилась новая форма преступной деятельности, использующая электронные ресурсы, а именно преступления в сфере компьютерной информации и мошенничество в сети Интернет. Мошенники ежегодно обманывают миллионы людей, используя интернет-сервисы или программное обеспечение. Эти мошенничества заставляют жертв отправлять деньги или предоставлять личную информацию. В настоящее время эти новые формы преступности растут и представляют собой новую и главную проблему для правоохранительных органов на всех уровнях, а именно в том, как предупреждать, расследовать и раскрывать эти преступления. Правоохранительные органы от местного до федерального уровня начинают создавать специальные подразделения, занимающиеся расследованием компьютерных преступлений, но в настоящее время не существует единого метода определения и устранения преступлений в сфере компьютерной информации и мошенничества в сети Интернет.

Уголовный кодекс Российской Федерации содержит четыре состава, называемых преступлениями в области компьютерной информации. К ним относятся:

- неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);

- неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ).

Данные преступления на первый взгляд достаточно схожи, но при правильной трактовке каждой из статей они образуют совершенно разные преступления, за которые предусмотрена различная ответственность.

И.А. Клепицкий пишет, что предметом компьютерных преступлений является автоматизированная система обработки данных, которая включает как материальный элемент (ЭВМ и сетевое оборудование), так и элемент нематериальный (программы и иная информация) [2].

Стоит уточнить, что данное утверждение требует особой оговорки, исходя из последних законодательных изменений.

На мой взгляд, предметом преступлений в сфере компьютерной информации по ст. 272-274 Уголовного кодекса Российской Федерации может являться исключительно компьютерная информация, хотя компьютерная информация не может существовать вне компьютера, компьютерного носителя информации, компьютерной сети или каналов связи.

Рассмотрим главные отличия статей главы 28 Уголовного Кодекса между собой.

Начнём со статьи 272 – неправомерный доступ к компьютерной информации.

Чтобы применить эту статью, недостаточно войти в компьютерный носитель, компьютер, компьютерную систему или компьютерную сеть (например, для чтения информации). Конструктивным признаком, при отсутствии которого не образуется преступление, является совершение определенного действия или начало расследования, прямо предусмотренного законом. То есть оформление объективной стороны состава предполагает не только ознакомление с информацией, но и ее обязательную незаконную обработку путем совершения противоправного действия: либо уничтожения, либо блокирования, либо изменения, либо копирования информации [3]. Это преступление может быть совершено как умышленно, так и по неосторожности.

Далее рассмотрим статью 273 – создание, использование и распространение вредоносных компьютерных программ.

Ответственность устанавливается за сам факт создания, распространения или же использования вредоносных компьютерных программ или иной компьютерной информации. Для признания такого деяния оконченным не требуется наступление последствий. Однако если создание, распространение или использование программы для ЭВМ или иной компьютерной информации, повлекшее уничтожение, блокирование, изменение или копирование информации, выступает в качестве дополнительного элемента деяния при наличии всех необходимых признаков преступления, в частности вины, то оно может быть квалифицировано по статье 272 УК РФ [3]. Это преступление может быть совершено только с прямым умыслом.

Следующая рассматриваемая статья – 274 – нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Здесь необходимо обратить внимание на то, что нарушение правил эксплуатации средств хранения, обработки или же передачи компьютерной информации или информационно-телекоммуникационных сетей и терминального оборудования, а также правил доступа к информационно-телекоммуникационным сетям влечет за собой не только последствия в виде уничтожения, блокирования, изменения или копирования охраняемой законом информации, но и должно выражаться в причинении крупного ущерба. Факт уничтожения или блокирования информации в результате нарушения правил работы по данной статье не наказуем [3]. Это преступление может быть совершено как умышленно, так и по неосторожности.

Последней статьей в этой главе является относительно новая статья 274.1 – неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

В ст. 274.1 УК РФ можно выделить три самостоятельных состава преступления по частям этой статьи.

Ч. 1 ст. 274.1 схожа по составу со ст. 273 УК, но важно разграничить данные статьи по цели совершения преступления. В рассматриваемой статье целью будет являться неправомерное воздействие именно на критическую информационную инфраструктуру Российской Федерации, а при квалификации статьи 273 цель не имеет значения.

Ч. 2 ст. 274.1 установлена уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации. Данный состав следует отличать от состава, предусмотренного ст. 272 УК РФ, по признакам объективной и субъективной стороны.

Ч. 3 ст. 274.1 устанавливает ответственность за нарушение правил, которые повлекли причинение критической информационной инфраструктуре Российской Федерации вреда. Может характеризоваться как умыслом, так и неосторожностью по отношению к наступившим последствиям.

Составы преступлений, изложенные выше, следует отграничивать от схожего преступления, а именно предусмотренного статьей 159.6 – мошенничество в сфере компьютерной информации.

Это деяние определяется как хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, изменения компьютерной информации или иного вмешательства в работу средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Пленум Верховного Суда РФ счел важным уточнить, что для квалификации должны присутствовать все перечисленные в настоящей статье приемы, а именно: ввод, удаление, блокирование, изменение компьютерной информации и иное вмешательство [1].

Компьютерная информация применительно к статье 159.6 УК РФ – это информация, зафиксированная на машинном носителе или передаваемая по телекоммуникационным каналам в форме, доступной восприятию ЭВМ [4].

Данное преступление разграничивается с преступлениями, предусмотренными главой 28 Уголовного кодекса, по следующим основаниям:

- перечень признаков, перечисленных в ст. 159.6 шире, чем тот, который приведён в ст. 272;

- по направленности умысла – по ст. 159.6 умысел направлен на хищение чужого имущества;

- для привлечения к уголовной ответственности по данной статье минимальная сумма причинённого вреда ниже, чем по составам главы 28 Уголовного кодекса;

- для квалификации по ст. 272, 273 необходим мотив в виде корыстной заинтересованности;

- иное.

По данным судебной статистики, в 2019 году по статье 159.6 было осуждено 34 человека, из них лишены свободы 10 человек, в 2018 году осуждены 54 человека, лишены свободы 15, в 2017 году осуждено 144 человека, лишены свободы 49 человек.

По статье 272 в 2019 году было осуждено 85 человек, из них лишены свободы 3 человека, в 2018 году осуждены 50 человек, лишены свободы 2 человека, в 2017 году осуждено 74, из них лишено свободы 9 человек.

По статье 273 в 2019 году были осуждены 76 человек, из них лишены свободы 4, в 2018 году осуждены 79, лишен свободы 1 человек, в 2017 году из 128 осуждённых были приговорены к лишению свободы 4 человека.

По статье 274 в 2019, 2018 и 2017 годах статистика не менялась и была нулевой.

По статье 274.1 в 2019 году было осуждено 4 человека, в 2018 и 2017 годах статистика нулевая, это связано с новизной данной нормы [5].

Исходя из статистики, можно выявить тот факт, что данные преступления совершаются достаточно редко и чаще всего такой вид наказания, как лишение свободы не применяется. Также можно сделать вывод по ст. 274, чья статистика не меняется на протяжении трёх лет, что может говорить о том, что данная норма достаточно сложна для применения и требует разъяснения вышестоящими инстанциями по поводу ее применения.

Библиографический список

1. Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. №48 «О судебной практике по делам о мошенничестве, присвоении и растрате». [Электронный ресурс] URL: https://rg.ru/2017/12/11/sud-moshennichestv-dok.html. Дата обращения: 23.11.2020.

2. Уголовное право Российской Федерации. Особенная часть / под ред. Б.В. Здравомыслова. М.: Юристъ, 2000. 552 с.

3. Попов А.Н. Преступления в сфере компьютерной информации. СПб.: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 68 с.

4. Комментарий к ст. 159.6 Уголовного кодекса РФ [Электронный ресурс]. URL: http://stykrf.ru/159-6 (дата обращения: 24.11.2020).

5. Информационный портал [Электронный ресурс]. URL: stat.апи-пресс.рф (дата обращения: 25.11.2020).

DISTINGUISHING INTERNET FRAUD FROM RELATED CRIMES IN THE FIELD OF COMPUTER INFORMATION

Yakovleva Ya.Yu.

Scientific adviser: Inyushkin A.A.

Samara National Research University, Samara, Russia

Abstract. *The article deals with crimes on the Internet and in the field of computer information. The differences between the corpus delicti are given. The features of each of the articles of these crimes are highlighted. The statistics on art. 159.6, 272, 273, 274 and 274.1.*

Keywords: *Internet fraud, crimes in the field of computer information, delimitation of crimes, computer information.*