DOI 10.37539/2949-1991.2023.6.6.010

Нерсесян Артур Варданович,
студент 3 курса, Юридического факультета им. А.А. Хмырова,
ФГБОУ ВО «Кубанский государственный университет», г. Краснодар

Научный руководитель:
Куфлева Валентина Николаевна, кандидат юридических наук,
доцент кафедры уголовного права и криминологии
Кубанского государственного университета, г. Краснодар

КИБЕРПРЕСТУПНОСТЬ: ТЕКУЩИЕ ТРЕНДЫ И ВЫЗОВЫ
CYBERCRIME: CURRENT TRENDS AND CHALLENGES

Аннотация: Статья представляет собой обзор и анализ текущей ситуации в сфере киберпреступности. В статье рассматриваются понятие киберпреступности, последние тренды и новые методы, которые используются киберпреступниками, а также проблемы, с которыми в настоящее время сталкиваются правоохранительные органы.

Abstract: The article is an overview and analysis of the current situation in the field of cybercrime. The article discusses the concept of cybercrime, the latest trends and new methods used by cybercriminals, as well as the problems currently faced by law enforcement agencies.

Ключевые слова: киберпреступность, кибербезопасность, преступления в сфере компьютерной информации.

Keywords: cybercrime, cybersecurity, crimes in the field of computer information.

Введение понятия «киберпреступние» в Уголовный кодекс Российской Федерации уже несколько лет является предметом споров. Отчасти это связано с тем, что Россия, как и многие другие страны, пытается угнаться

за стремительными изменениями, которые привносят в нашу жизнь технологии. Важно понимать, что с расширением доступа к цифровым ресурсам и сетям наблюдается экспоненциальный рост киберпреступности, поскольку преступники направляют свои усилия на использование этих ресурсов для совершения широкого спектра преступных действий. Цифровизация и внедрение технологий научно-технического прогресса в жизнь общества, с одной стороны, упростили многие жизненные процессы, но, с другой стороны, сделали людей и государство более уязвимыми, что явилось обстоятельством возникновения киберпреступности, кибертерроризма, киберэкстремизма.

Киберпреступность – это деяние, которое не имеет территориальных границ, оно может происходить везде, где люди используют IT-устройства. В связи с этим, исследование проблемы отсутствия дефиниции «киберпреступление» в уголовном законодательстве РФ является актуальным. Киберпреступность можно определить, как совокупность преступлений, совершаемых в киберпространстве (информационном пространстве) с помощью или посредством компьютерных систем или компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей и против компьютерных систем, компьютерных сетей и компьютерных данных. [1] Киберпреступлением, в свою очередь, можно признать совокупность незаконных действий, совершаемых с использованием информационных технологий и цифровой среды, нарушающих нормы уголовного закона и причиняющих ущерб правам, интересам и защите персональной информации физических или юридических лиц.

Она имеет ряд черт, которые не свойственны традиционной преступности: повсеместное использование шифрования и дистанционность доступа к предмету посягательства; сложность с фиксацией доказательств; не традиционность способов совершения преступления; отсутствие должных механизмов контроля в силу несовершенства обеспечения информационной безопасности в киберпространстве. [2]

Необходимо подходить к вопросу противодействия киберпреступности с полной ответственностью, поскольку в настоящее время киберпреступность стала профессиональной, высокотехнологичной, с использованием искусственного интеллекта и широкого спектра инструментов.

Использование искусственного интеллекта в целях распространения вирусов в современной научной теории именуется, как анекселенктотичная технотронная преступность, то есть, иными словами, вид преступности, который основан на использовании современных технологий без как такового управляемого процесса заражения. [3]

Высокотехнологичная технотронная преступность вытесняет традиционную компьютерную преступность, создавая новую систему общественно опасных деяний, основанных на использовании компьютерных, информационно-коммуникационных, космических и других разработках.

Киберпреступность может быть направлена не только на уничтожение информации, но и на приведение в негодность различного вида оборудований, что, в конечном счете, может нанести вред экономике государства, предприятиям, объектам критической информационной инфраструктуры, здоровью и жизни людей.

Согласно данным, представленным на официальном сайте МВД РФ, каждое четвертое преступление совершается с использованием высоких технологий, что свидетельствует о распространении криминальных процессов с использованием киберпространства. [4]

В настоящее время законодательное регулирование киберпреступности основывается на таких нормативных правовых актах, как:

1. Доктрина информационной безопасности России, утверждённая Указом Президента РФ 5 декабря 2016 г. № 646, которая раскрывает дефиницию информационной безопасности Российской Федерации, под которой понимается такое состояние защищенности государства, общества и личности от информационных угроз, проявляющихся, как внутренне, так и

внешне, при котором обеспечиваются положения Конституции Российской Федерации, реализуются права и свободы человека и гражданина, обеспечивается достойный уровень жизни граждан, а также оборона и безопасность страны. [5]

2. В соответствии с Федеральным законом от 27 июля 2006 г. № 149-ФЗ (ред. от 30 декабря 2021 г.) «Об информации, информационных технологиях и о защите информации» защита информации включает правовые, организационные и технические меры, которые призваны не допустить неправомерный доступ, уничтожение, модификацию, блокировку, копирование информации и другие технические неправомерные действия по отношению к ней; соблюдать конфиденциальность в отношении информации ограниченного пользования. [6]

Стоит отметить, что в настоящее время, Концепция стратегии кибербезопасности не разработана должным образом, чтобы быть принятой на законодательном уровне. Однако, в целях соответствия современному развитию общества и научно-технического прогресса необходимость включения самостоятельной дефиниции «киберпреступление» является необходимой мерой, поскольку ни один действующий нормативный правовой акт не раскрывает в должной мере данный термин и не отвечает современным методам противодействия киберпреступности. Считаем, что только комплексный подход теории и практики может привести к прогрессивным результатам в борьбе с киберпреступностью.

УК РФ содержит гл. 28 «Преступления в сфере компьютерной информации», которая находится в разделе IX «Преступления против общественной безопасности и общественного порядка».

В данном случае, объектом компьютерных преступлений выступают общественные отношения, связанные с защитой информации неопределенного вида. Следовательно, сама информация раскрывается в широком понимании дефиниции и является часть общественной безопасности.

В примечании к ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» даётся понятие компьютерной информации, под которой понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. [7]

Вместе с тем более, полагаем конкретизировано понятие информации в ст. 5 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: информация может являться объектом публичных, гражданских и иных правовых отношений; информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку её предоставления или распространения. [8]

Исходя из данной дефиниции можно сделать вывод, что информация является промежуточным звеном, мерой связи между событием и объективными изменениями, которое вызвало данное событие.

Как указал ВС РФ, термин «электрический сигнал» в примечании к ст. 272 УК РФ является неопределенным и требует внесения разъяснений. [9]

Стоит отметить, что в русской лексике и терминологии, относительно компьютерных и информационных элементов, процессов, технологий, происходит смешивание английского и русского языков. Так, к примеру, логин (англ. login), PIN-код (англ. pin) и др.

Относительно дефиниции «Компьютерные преступления» в науке существуют различные мнения. [10,11] Однако, компьютер нельзя рассматривать, как объект, против которого совершается преступление, поскольку компьютер является техническим средством для работы с информацией. При квалификации компьютерных преступлений необходимо обращать внимание вид информации, к которой осуществляется неправомерный доступ, на ее свойства и характеристику, а также на то, какое действие в отношении нее было совершено: уничтожение, блокирование, модификация, копирование.

Возвращаясь к ст. 272 УК РФ, считаем, что предметом преступления, предусмотренного ст. 272 УК РФ, является любая информация, принадлежащая конкретному лицу, закреплённая на любом электронном носителе или передаваемая в качестве электрического сигнала, которую уничтожают, блокируют или оказывают иное вредное воздействие, в результате чего её невозможно в дальнейшем использовать или воспроизвести.

Если рассматривать ст. 272 УК РФ с позиции юридической техники, само название статьи не соответствует своему содержанию, поскольку наименование исходит из того, что происходит неправомерный доступ к охраняемой компьютерной информации, однако диспозиция статьи раскрывается с помощью наличия обязательных условий, при которых деяние становится общественно опасным.

Предлагаем под компьютерной информацией считать зафиксированные на материальном носителе сведения (сообщения, данные, команды), представленные в виде, пригодном для обработки с использованием компьютерных устройств, и предназначенные для использования в таких устройствах.

Придерживаемся мнения, что в УК РФ название главы «Преступления в сфере компьютерной информации» является устаревшим и требует изменения (например, «Преступления в сфере информационных технологий») или корректировки, поскольку такие преступления могут совершаться не только с помощью компьютера, но и с помощью любых электронных носителей и средств связи.

Считаем, что в целях обеспечения должной общественной и национальной безопасности страны от киберпреступлений необходимо строить новую концептуальную систему законодательства, избегая разрозненности в наименовании документов стратегического планирования и государственного регулирования.

На сегодняшний день имеют распространение DDoS-атаки, направленные в целях целенаправленной перегрузки серверов или сетевых компонентов. Сам термин DDoS означает «распределенный отказ в обслуживании», т.е. промежуточная цель заключается в том, чтобы сделать определенную систему недоступной. В данном случае применяется ст. 273 УК РФ, однако, преступник несет наказание только за распространение вредоносных компьютерных программ, хотя конечная цель может быть совершенно другой – начиная от нанесения ущерба репутации, заканчивая полным отключением сайта в целях нанесения материального ущерба владельцам электронного ресурса. [12]

Также необходимо сделать акцент на одном из современных видов киберпреступлений – кибербуллинге. В российском законодательстве данный термин отсутствует, что, опять же, порождает споры относительно дефиниции данного термина. Кибербуллинг проявляется путем психологического воздействия (ощущения постоянного чувства страха) на жертву или агрессивного поведения в информационной среде в целях травли выбранной жертвы, распространения клеветы, оскорблений, доведения до самоубийства, кибепреследования с последующей организацией вымогательства, шантажа и др. [13] Общественная опасность данного преступления очевидна и соответствует сегодняшним реалиям, и мы придерживаемся позиции, что кибербуллинг должен быть закреплен в УК РФ, как состав преступления и в должной мере оценен с позиции меры наказания.

Аккумулируя изложенное, отметим, что отсутствие качественного реагирования на киберпреступность может привести к уменьшению контроля в сфере национальной безопасности страны и возникновению новых угроз. Необходимо подходить к данному явлению не только с законодательной стороны, но и с позиции подготовки квалифицированных сотрудников правоохранительных органов.

Список литературы:

1. Номоконов В.А., Тропина Т.Л. Киберпреступность как новая криминальная угроза // Криминология вчера, сегодня, завтра. 2012. № 1 (24). С. 96.

2. Винкерт В.В., Клочкова А.Л. Понятие и особенности киберпреступлений // Междисциплинарные исследования: опыт прошлого, возможности настоящего, стратегии будущего. 2021. №5. URL: https://cyberleninka.ru/article/n/ponyatie-i-osobennosti-kiberprestupleniy (дата обращения: 26.03.2023).

3. Евдокимов К.Н. Анекселенктотичная технотронная преступность (частная теория) // Уголовное право и процесс. 2018. № 4. С. 35–39.

4. Министерство внутренних дел Российской Федерации // Официальный сайт. URL: https://xn--b1aew.xn--p1ai/reports/item/35396677/ (дата обращения 06.03.2023).

5. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 // Собрание законодательства РФ, 12.12.2016, № 50, ст. 7074.

6. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.03.2023) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

7. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 № 63-ФЗ (ред. от 10.07.2023) // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

8. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 01.03.2023) // Собрание законодательства РФ, 31.07.2006, № 31 (1 ч.), ст. 3448.

9. Отзыв Верховного Суда Российской Федерации на проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» от 7 апреля 2011 г. № 1/общ-1583 // Доступ из ИПП «Гарант». URL: https://www.garant.ru/article/520694/ (дата обращения: 26.03.2023).

10. Чакрян В. Р., Кешишян В. В. Понятие компьютерных преступлений и их классификация // Символ науки. 2020. №12-2. С. 71;

11. Скляров С. В, Евдокимов К. Н. Современные подходы к определению понятия, структуры и сущности компьютерной преступности в Российской Федерации // Всероссийский криминологический журнал. 2016. №2. С. 2.

12. Антонова Т.С., Смирнов В.М. Фишинг как неизученное киберпреступление // StudNet. 2021. №6. URL: https://cyberleninka.ru/article/n/fishing-kak-neizuchennoe-kiberprestuplenie (дата обращения: 26.03.2023).

13. Бочкарева Е.В., Стренин Д.А. Теоретико-правовые аспекты кибербуллинга // Всероссийский криминологический журнал. 2021. №1. URL: https://cyberleninka.ru/article/n/teoretiko-pravovye-aspekty-kiberbullinga (дата обращения: 26.03.2023).