Шарыпова Т.Н.,
кандидат экономических наук
доцент кафедры информационных технологий и защиты информации
Ростовский государственный экономический университет «РИНХ»
Россия, г. Ростов-на-Дону
Сидоренко А.А.,
студент, 1 курс юридический факультет
Ростовский государственный экономический университет «РИНХ»
Россия, г. Ростов-на-Дону

КИБЕРПРЕСТУПНОСТЬ В XXI ВЕКЕ

Аннотация: *в статье рассматривается одна из проблем современного общества – киберпреступность. Проводится анализ ее динамики, а также оценка несовершенства российского законодательства, регулирующего отношения в сети Интернет.*

Ключевые слова: *киберпреступность, мошенничество, информационное общество, законодательство юридическая ответственность.*

Annotation: *the article deals with one of the most serious problems of modern society – cybercrime. The paper analyzes its dynamics and assesses the imperfection of the Russian legislation regulating relations on the Internet.*

Keywords: *cybercrime, fraud, information society, legislation legal responsibility.*

Киберпреступность — это преступность в так называемом виртуальном пространстве. Киберпространство можно определить как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленных в математическом, символьном или любом другом виде ,и находящихся в процессе движения по локальным и глобальным компьютерным

сетям, либо сведения, хранящиеся в памяти любого реального или виртуального устройства, а также другого носителя, специально предназначенного для их хранения, обработки и передачи. [1]

Термин «киберпреступность» включает в себя любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети. Преступление, совершенное в киберпространстве, — это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация цифровых данных, а также иные противоправные общественно опасные действия, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ.[1]

Сегодня киберпреступность в Российской Федерации и других странах характеризуется довольно быстрой динамикой развития. Киберпреступность представляет собой любое преступление, совершенное в виртуальном пространстве с помощью информационно-коммуникационных технологий (ИТК). С каждым годом число киберпреступлений и, следовательно, число жертв таких преступлений постоянно увеличивается.

Главная причина увеличения числа киберпреступлений в основном связано с тем, что Интернет в современном мире имеет большое значение. На растущее число преступлений из года в год, совершаемых в сети Интернет, также влияет тот факт, что огромное количество различной информации хранится именно в электронном виде. Кроме того, в настоящее время широко распространены электронные платежи, которые чаще всего подвергаются атакам различными хакерами.

Сегодня в мире распространена практика использования в личных целях услуги, предоставляемой киберпреступниками. Так, самой распространенной услугой является предоставление несанкционированного доступа к личной информации какого-либо человека, компании (например, учетным записям в разных социальных сетях и электронной почте) [5].

Так, согласно результатам ежегодного исследования, которое проводится компанией «Symantec», в 2018 году в мире 980 миллионов пользователей сети Интернет пострадали от незаконных действий со стороны киберпреступников, в результате чего было украдено порядка 172 миллиарда долларов США [1].

Социологи, проводившие данные исследования, пришли к выводу, что жертвами хакеров в основном являются люди, которые используют большое количество коммуникационных устройств в повседневной жизни или на работе, и имеющие слабое представление об основах безопасности в сети Интернет или же вообще не имеют такого представления. Как правило, эти пользователи устанавливают один и тот же пароль для доступа к разным учетным записям и в то же время могут делиться этим паролем с другими людьми.

Согласно результатам исследования, сегодня порядка 20 пользователей старше 18 лет по истечению одной секунды становятся жертвами мошенников в сети Интернет, и так, более 1,5 миллиона человек во всем мире ежедневно [2]. В лучшем случае средний вред, нанесенный кибератакой мошенников на обычного пользователя, составляет около 200 долларов США [1].

В России с 2016 по 2018 год количество преступлений увеличилось в 6 раз (с 11 000 до 66 000). Рост атак наиболее был высок в 2018 году и достиг 40 тысяч [3].

Согласно официальной статистике, в России в первом полугодии 2018 года ущерб от киберпреступности составил порядка 18 миллионов долларов США. Так, по данным прокуратуры Российской Федерации, наиболее распространенными преступлениями в сети Интернет являются различные информационные барьеры, компьютерный шпионаж и ряд других опасных атак [2].

Сегодня, Интернет, ввиду практической безнаказанности, широко используется для продвижения различных экстремистских идей и движений. Например, в 2018 году в Российской Федерации 2/3 всех преступлений экстремистской направленности было совершено с использованием Интернета [3].

Чтобы бороться с киберпреступностью, а также эффективно предотвращать различные интернет-преступления, необходимо принять ряд мер, направленных непосредственно на предотвращение противоправных действий в сети Интернет. Одна из таких мер должна заключаться в совершенствовании законодательства в Российской Федерации.

29 ноября 2012 года был принят Федеральный закон № 207-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и некоторые законодательные акты Российской Федерации» в результате принятия окончательно определились конкретные виды мошенничества, что позволило их отнести к тем или иным составам преступлений. Так, появилась статья 159.3 УК РФ «Мошенничество с использованием платежных карт», а также статья 159.6 УК РФ «Мошенничество в сфере компьютерной информации» [5].

В настоящее время существует много проблем, связанных с предотвращением мошенничества в сети Интернет. Это:

1) слабая нормативно-правовая база в компьютерной криминалистике;

2) нежелание правоохранительных органов расследовать преступления категории интернет-преступления;

3) отсутствие компетентных специалистов в правоохранительных органах, которые своими действиями могут предотвратить различные хакерские преступления.

Несмотря на то, что российское законодательство, регулирующее виртуальное пространство постоянно совершенствуется, это не позволяет в полной мере решить все проблемы, возникающие в результате киберпреступлений.

Таким образом, сегодня киберпреступность несет в себе серьезную общественную опасность, которая не в полной мере осознана как российским законодательством, так и законодательством других стран. В настоящее время в Российской Федерации существует несоответствие между ущербом, причиненным киберпреступностью, и наказанием за такой ущерб, что требует

пересмотра всей юридической ответственности за правонарушения в сети Интернет.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Ширяева С. Н. Моббинг как направление в криминологической науке // Молодой ученый. 2014. № 6-1 (65). С. 42 – 43

2. 2018 Norton Cyber Security Insights Report // Symantec. URL: https://www.symantec.com/about/newsroom/press-kits/ncsir-2018 (дата обращения: 05.01.2019).

3. Число киберпреступлений в России выросло за 3 года в 6 раз // Интерфакс. URL: http://www.interfax.ru/russia/576166 (дата обращения: 05.01.2019).

4. Ландик С.А., Шарыпова Т.Н. Компьютерные преступления и мероприятия по защите электронных данных. В сборнике: наука сегодня: вызовы и решения, материалы международной научно-практической конференции: в 2 частях. 2018. С. 68-70.

5. Тищенко Е.Н., Шарыпова Т.Н. Формализация выбора различных вариантов системы защиты информации от несанкционированного доступа в среде электронного документооборота. Вестник Ростовского государственного экономического университета (РИНХ). 2010. № 3 (32). С. 226-233.

6. Уголовный кодекс РФ.