УДК 34.06

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

КИБЕРПРЕСТУПЛЕНИЯ. ЦЕЛИ, ПОСЛЕДСТВИЯ И МЕТОДЫ ЗАЩИТЫ

Аннотация: *в статье рассматривается такая проблема современного общества, как киберпреступность. Каждый год в мире количество киберпреступлений растет. Это связано с постоянным техническим развитием компьютерных и информационных технологий, которые, в свою очередь, помогают преступникам создавать все новые и новые способы и средства обхода защитных систем.*

Ключевые слова: *киберпреступность, кибермошенничество, кибербезопасность, виртуальное пространство.*

Sharypova T.N.
Associate Professor of the Department of Information Technologies and Protection
Rostov State University of Economics
Russia, Rostov-on-Don
Sivakov V.N.
student1 year, Faculty of Law

Rostov State University of Economics

Russia, Rostov-on-Don

CYBER CRIME. GOALS, CONSEQUENCES AND METHODS OF PROTECTION

Abstract: *this article deals with such a problem of modern society as cybercrime. Every year in the world the number of cybercrime grows. This is due to the constant technical development of computer and information technologies, which, in turn, help criminals to create more and more new ways and means of circumventing protective systems.*

Key words: *cybercrime, cyber fraud, cyber security, virtual space.*

Киберпреступность – это преступления в виртуальное пространство. К такому роду преступлений относится кража данных банковских карт, распространение вредоносного программного обеспечения, фишинг (кража конфиденциальной информации), распространение запрещенного контента (клевета и материалы, разжигающие межрелигиозную и межрелигиозную вражду), а также вмешательство в сеть различных частных и коммерческих компьютерных систем.

Потенциальными жертвами этого вида преступлений могут быть не только выдающиеся бизнесмены или политики, но также дети и пожилые люди. В этом случае, как правило, нарушитель и его цель находятся за тысячи километров друг от друга [1].

Наиболее распространенными целями киберпреступности являются:

1) незаконное получение денежных средств, ценных бумаг, кредитов, физических ценностей, товаров и услуг, концессий, льгот, квот, недвижимости, топлива, сырья, энергоресурсов и стратегического сырья;

2) уклонение от уплаты налогов, сборов, пошлин и т.д.;

3) криминализация (отмывание) доходов, полученных преступным путем;

4) подделка или изготовление поддельных документов, штампов, штампов, макетов, кассовых билетов для личной выгоды;

5) доступ к конфиденциальной информации в корыстных или политических целях и множество других.

Хакеры совершают преступления в основном с помощью вредоносных программ. Так наиболее распространенным способом является использование компьютерных файловых вирусов, которые вводят свой вредоносный код в программный код различных файлов. Также популярным среди преступников является заражение мобильных устройств троянцами с помощью SMS или почты [2].

Сегодня преступники все чаще наносят ущерб частным компаниям, правительственным учреждениям и простым людям. Так, каждый год, согласно отчету международного агентства безопасности, в области киберугроз – «Symantec Security», в 1 секунду в мире происходит 12 кибератак, что составляет 556 миллионов киберпреступлений в год. Общий ущерб от них оценивается в 100 миллиардов долларов США. Так, по данным «Лаборатории Касперского», только в третьем квартале 2018 года было отражено 947027517 атак из 185 стран [4].

Ущерб крупнейших российских банков (Сбербанк, Альфа-Банк и другие) от кибератак за 2018 год составил более 1 млрд. рублей. В атаке участвовали тысячи компьютеров со всего мира. В 2017 же году также были атакованы электронные почты 57 миллионов пользователей «Mail.ru», 40 миллионов «Yahoo», 33 миллиона «Hotmail» и 24 миллиона «Gmail». В общей сложности пользователи потеряли около 272 миллиона личных данных [5].

12 мая 2017 года произошла одна из крупнейших кибератак с использованием вредоносной программы «WannaCry», которая затронула только устройства, работающие на «Microsoft Windows». Сначала была атакована Испания, затем другие страны. Россия заняла первое место по количеству жертв. Программа поразила более 500000 компьютеров правительственных учреждений, коммерческих организаций и частных лиц. Результатом атаки стало

шифрование данных и требование от ее пользователей выплат в размере 300-600 долларов США, под угрозой удаления всей зараженной информации [5].

Киберпреступность в России и мире с каждым годом становится все популярнее из-за безнаказанности. Успехи в борьбе с угрозами такого типа необходимы для того, чтобы привести составы киберпреступлений в Уголовный кодекс Российской Федерации. Нынешние статьи 272, 273 и 274 не учитывают современные технологические особенности, а наказание не соответствует тяжести преступлений. Также необходимы профилактические беседы с населением, чтобы подтолкнуть людей к наличию скрытой угрозы в Интернете. Основными методами защиты от киберпреступности являются:

1) не доверять «друзьям», которых мы не знаем в реальной жизни, а только через социальные сети;

2) своевременное обновление программного обеспечения (ПО) всех устройств;

3) использование надежных паролей в различных аккаунтах;

4) не использовать программы, ссылки, информацию от незнакомых лиц и многое другое.

Что касается корпоративной безопасности, то сегодня она включает в себя множество различных аспектов, таких как: контроль, идентификацию и регистрацию доступа внутренних пользователей компании к ресурсам и данным компании, обеспечение целостности, конфиденциальности и надежности отправляемых данных, контроль процедур информационной безопасности, защиту от несанкционированного доступа из внешних сетей и др. [3].

Сегодняшний рост компьютерных преступлений обусловлен их доходностью и минимальным риском. Рост числа киберугроз, несомненно, будет расти, и именно поэтому данная проблема должна быть в приоритете у рядовых граждан, компаний и государства в целом.

ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. 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.

2. Парфеленко А.А., Шарыпова Т.Н. Интернет-пиратство. В сборнике: наука сегодня: вызовы и решения, материалы международной научно-практической конференции: в 2 частях. 2018. С. 48-50.

3. 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.

4. Официальный сайт Лаборатории Касперского [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/ (дата обращения: 23.12.18).

5. Состояние преступности в Российской Федерации [Электронный ресурс]. – Режим доступа: https://xn--b1aew.xn--p1ai/folder/101762 (дата обращения: 23.12.18).Информация; тел- 8 (918) 548-33-04.