*УДК 004*

***Мирошниченко В.А.,***
***студент, 1 курс юридический факультет***
***Ростовский государственный экономический университет «РИНХ»***
***Россия, г. Ростов-на-Дону***
***Шарыпова В.А.,***
***студент 3 курс ФИИТ***
***Институт математики, механики и компьютерных наук***
***имени И.И. Воровича ЮФУ***
***Россия г. Ростов на Дону***

# КИБЕРПРЕСТУПЛЕНИЯ И СПОСОБЫ ИХ СОВЕРШЕНИЯ

***Аннотация:*** *в статье рассматривается такая проблема современного общества, как киберпреступность. Каждый год во всём мире значительно увеличивается число киберпреступлений. Это связано с непрерывным техническим развитием компьютерных и информационных технологий.*

***Ключевые слова:*** *киберпреступления, компьютерный вирус, виртуальное пространство, кибероружие, кибербезопасность.*

***Annotation:*** *the article deals with such a problem of modern society as cybercrime. Every year throughout the world, the number of cybercrime increases significantly. This is due to the constant technical development of computer and information technologies.*

***Keywords:*** *cybercrime, computer virus, virtual space, cyber weapon, cyber security.*

Для того чтобы начать говорить о киберпреступности, следует разобраться, что же такое компьютерный вирус и как он способствует совершению киберпреступлений.

Компьютерный вирус - вид вредоносного программного обеспечения, способный создавать копии самого себя, внедряться в код других программ, в системные области памяти, в загрузочные секторы, а также распространять свои копии по каналам связи [5].

Хакеры придумывают всё более сложные вирусы, а те, кто с ними борются, наращивают всё более сложную защиту.

Существуют самые массовые угрозы, с которыми человечество сталкивается каждый день, это черви, трояны, фишинговые письма и большинство атак в сети Интернет; также существуют целевые атаки, нацеленные на конкретных людей или организации; а новинкой нашего столетия является кибероружие. Каждый хакер сам решает, какую нишу ему занять и начинает бесконечную войну со специалистами по кибербезопасности [3].

Таким образом, киберпреступность - это преступность в виртуальном пространстве. Виртуальное пространство можно определить, как моделируемое с помощью компьютера информационное пространство, в котором находятся сведения о лицах, предметах, фактах, событиях, явлениях и процессах, представленные в математическом, символьном или любом другом виде и находящиеся в процессе движения по локальным и глобальным компьютерным сетям [1].

Рассмотрим способы совершения киберпреступлений: фишинг, спам, инсайдинг, хакерство, похищение цифровой личности, телекоммуникационные преступления.

1. Фишинг - это один из способов интернет мошенничества, когда всеми возможными правдами и неправдами пытаются узнать различные персональные

данные (пароли, логины, номера банковских карт и счетов). Смысл заключается в том, чтобы побудить перейти по фишинговый ссылке на поддельную страницу, визуально похожую на настоящую, например, банка, где под различными предлогами выудить персональную информацию.

2. Спам. К нему относятся нежелательные рекламные объявления, мистификации и сообщения, предназначенные для распространения рекламных объявлений или вредоносных программ. Доставляемые пользователю неудобства и опасность увеличиваются из-за того, что стоимость рассылки минимальна, а в распоряжении авторов спама есть множество средств получения новых адресов электронной почты и способов нелегально рассылать сообщения.

3. Инсайдинг. Инсайдер (работающий или освобожденный сотрудник компании) является потенциальным преступником. Знакомый с тонкостями компьютерной системы компании, он имеет неограниченный доступ к системе с целью незаконного вмешательства в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей, или с целью незаконного завладеет информацией, которая является собственностью компании.

4. Хакерство. Хакер чрезвычайно квалифицированный IT-специалист, человек, который понимает самые глубины работы компьютерных систем. Изначально хакерами называли программистов, которые исправляли ошибки в программном обеспечении каким-либо быстрым и далеко не всегда элегантным или профессиональным способом. Однако большинство людей считают, что хакер компьютерный взломщик, проникающий в закрытые информационные сети, банки данных и тому подобное с целью получения доступа к секретной информации, а также заражения их вирусами.

5. Похищение цифровой личности - неправомерное завладение, например, профилем в социальной сети, с целью рассылки спама, использования личных данных, шантажа, выманивания денежных средств и другое.

6. Телекоммуникационные преступления - преступления, совершаемые через СМИ и средства связи. Наиболее известным из них является атака с целью перегрузить оборудование жертвы и помешать его нормально использовать [2].

Для того чтобы обезопасить себя от киберпреступлений достаточно придерживаться следующих правил[4]:

- обязательно удаляйте скриншоты и сообщения с паролями, не сохраняйте пароли в браузерах;

- не переходите по подозрительным ссылкам;

- пользуйтесь приложениями, а не сайтами каких-либо магазинов, они безопаснее;

- не пересылайте фотографии своих банковских карт. Для получения перевода, достаточно шестнадцати цифр расположенных на лицевой стороне карты, а срок действия и код на обратной стороне карты рекомендуется держать при себе.

Таким образом, человек по-прежнему остаётся самым слабым звеном защиты и, судя по тому, с какой скоростью киберпреступность набирает актуальность, защита от кибератак необходима каждому пользователю, имеющему аккаунты в сети Интернет.

## ИСПОЛЬЗОВАННЫЕ ИСТОЧНИКИ

1. Шафрин Ю.А. 1500 основных понятий, терминов и практических советов для пользователей персональным компьютером. - М.: Дрофа, 2015. - 272 с.

2. Фридланд А.Я. Информатика и компьютерные технологии: Основные термины: Толков. Слов.: Более 1000 базовых понятий и терминов. - 3е изд. испр. и доп./ А.Я. Фридланд, Л.С. Ханамирова, И.А. Фридланд. - М.: ООО «Издательство Астрель», 2017. - 272 с.

3. 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.

4. 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.

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.