УДК 34

КИБЕРПРЕСТУПНОСТЬ КАК НОВАЯ КРИМИНАЛЬНАЯ УГРОЗА

Гридина Ю.А.
Студент 1 курса АП и НБ
ЧОУ ВО ЮУ (ИУБиП)
Русскова А.А.
Студент 1 курса АП и НБ
ЧОУ ВО ЮУ (ИУБиП)

Аннотация: В данной статье рассмотрена и проанализирована такая острая проблема, как развитие киберпреступности не только в Российской Федерации, но и в мире. Так же способы с киберпреступностью и защиты от злоумышленников в сети

Ключевые слова: киберпреступность, защита, киберпреступления, мошенники, сеть, интернет, хакеры, преступления

CYBERCRIME AS A NEW CRIMINAL THREAT

Gridina Yu. A.
Russkova A. A.

Аннотация: This article considers and analyzes such an acute problem as the development of cybercrime not only in the Russian Federation but also in the world. The same methods with cybercrime and protection from intruders in the network.

Keywords: cybercrime, protection, cybercrime, fraudsters, network, internet, hackers, crime.

В настоящее время интернет нередко используется для получения доступа к личной информации граждан, шпионажа, пропаганды ненависти и вражды. Как известно из судебной практике две трети правонарушений в сфере киберпреступности имеют экстремистскую направленность (ст. 282), а каждое девятое расценивается как террористическая деятельность. К сожалению, с каждым годом раскрыть преступления становить всё сложней и сложней. Поэтому мы должны придерживаться определенных правил для того, чтобы не попасться на уловки злоумышленников (хакеров.) Для того чтобы сохранить благополучие страны и сократить число экстремистских движений, нужно победить киберпреступность не только в самой стране, но и в мире.

Киберпреступностью является любая преступная активность [1,6], где объектом в качестве цели или инструмента является компьютер или сетевое устройство.

В некоторых киберпреступлениях осуществляются прямые атаки на компьютеры и другие устройства, которые способны вывести их из строя. В других - компьютеры используются в своих целях киберпреступниками для распространения вирусов, с помощью которых можно получить незаконную информацию, или криптовалюту.

Киберпреступники используют 4 способа для совершения операции [2,7].

1. Использование вредоносных программ.

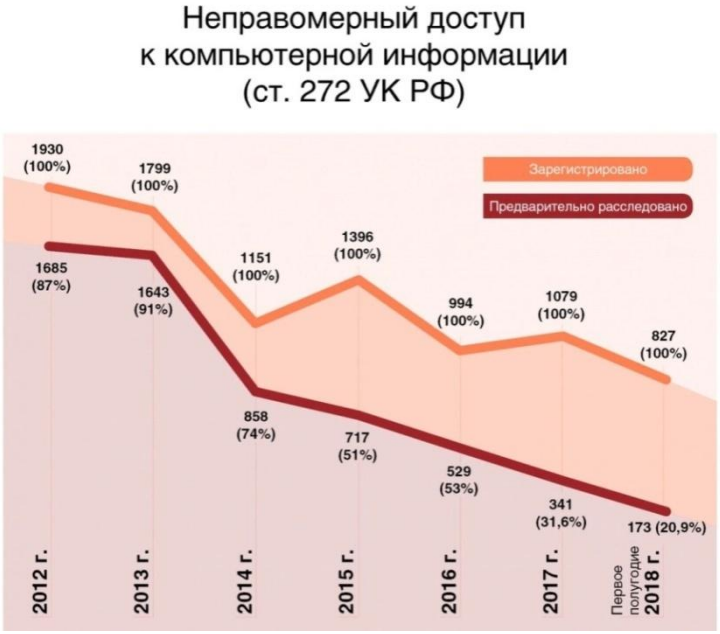
Данный способ не опасен для тех, кто использует антивирусные программы и сложные пароли.

2. DDOS атаки, когда злоумышленник пользуется коммуникационным сетевым протоколом для создания огромного количества запросов к серверу или службе. В этом типе атак главная цель – вывести из строя объект воздействия.

3. Комбинация социальной инженерии и вредоносного кода. Наиболее известная форма подобного рода атак – фишинг, когда жертву принуждают к определенным действиям (нажатию на ссылку в электронном письме, посещению сайта и т. д.), что впоследствии приводит к выходу из строя системы при помощи вирусов и вредоносных программ.

4. Незаконная деятельность: домогательства, распространение незаконного контента, груминг и т. д. В таких случаях злоумышленники скрывают свои следы через анонимные профайлы, шифрованные сообщения и другие подобные технологии.

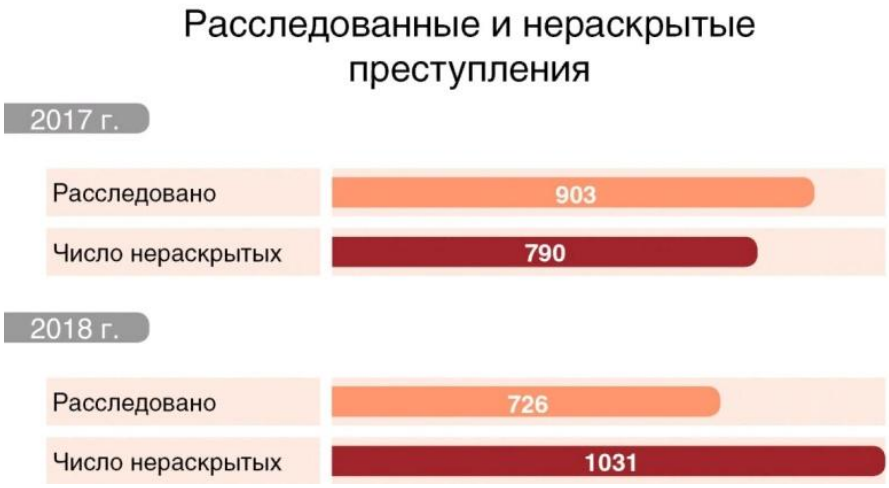
Как вы могли убедиться, киберпреступления включают в себя широкий диапазон незаконных деяний, начиная от мошенничества и кражи персональной информации и заканчивая преступлениями на почве ненависти и распространение наркотиков [3]. Между этими видами существуем множество пересечений, и сложно провести точную границу. Например, фишинговая атака может быть направлена на кражу персональной информации. Впоследствии, это может привести к подделке личности, которая будет использоваться для получения денег мошенниками, контрабандистами наркотиков или даже террористами. Важно понимать, что киберпреступления не всегда ассоциируются с изощренными схемами и не всегда затрагивают «глубокий интернет».



Если мы посмотрим на статистику с 2012 по 2018 год, то увидим, что неправомерный доступ к компьютерной информации снижается. Статистика показала, что злоумышленников стало почти в трое меньше.

Но опираясь на следующую статистику, можно сделать совсем другие выводы. Несмотря на снижение преступников, число нераскрытых

преступлений выросло, а это значит, что настало время не только устанавливать всем антивирусные программы, но и вовсе быть бдительными



и внимательными.

Интернет – это потрясающий инструмент для воплощения огромного количества идей! Однако, если вы действительно хотите что-то продать, лучше все-таки встретиться с покупателем лично. Итак, даже если вам удалось найти покупателя через Интернет, оплату лучше произвести в «реальном мире», чтобы удостовериться в подлинных намерениях покупателя.

Наказания за кибернарушения предусматривает глава 28 УК РФ. Она содержит 3 статьи, которые относятся к противоправным деяниям в сфере компьютерной информации – речь идёт о любых сведениях, существующих в виде электрических сигналов, независимо от средств их обработки, хранения или передачи [6]:

✓ Статья 272 УК РФ – утверждает наказание за незаконное получение доступа к кредитной истории, который привёл к блокированию, копированию, уничтожению или изменению данных. Уголовная ответственность предусмотрена вплоть до лишения свободы на срок до 7 лет.

- ✓ Статья 273 УК РФ – разработка, распространение, использование вредоносных программ. Срок наказания до 7 лет.
- ✓ Статья 274 УК РФ – нарушение требований к эксплуатации устройств для хранения, передачи и обработки данных компьютеров и телекоммуникационных информационных сетей. Предусматривает лишение свободы на срок до 5 лет.
- ✓ Другие статьи Уголовного кодекса, которые используются для противодействия преступникам, действующим в киберпространстве:
- ✓ Ч.3 и ч.6 ст.159 УК РФ Мошенничество с применением платёжных карт, а также противоправные деяния в сфере КИ, в том числе уничтожение или ввод данных.
- ✓ Ст. 146 Нарушение смежных и авторских прав при незаконном распространении Windows, других лицензионных программ и т. п.
- ✓ Ст. 242 Производство и оборот материалов и предметов порнографического характера.
- ✓ Ст. 138 Нарушение тайны переговоров по телефону, переписки, почтовых и других сообщений.
- ✓ Ст. 137 Неприкосновенность частной жизни.
- ✓ Ст. 282 Возбуждение вражды и ненависти, а также унижение человеческого достоинства.
- ✓ Ст. 183 Незаконное получение, разглашение информации, представляющей налоговую, коммерческую и банковскую тайну.
- ✓ Ст. 158 Кража.

Рассмотрев сущность понятия «киберпреступник» и как они действуют на протяжении 5 лет, как меняется статистика раскрытий киберпреступлений, можно сделать определённые выводы по борьбе с данным видом преступности. Нельзя забывать о том, что безопасность начинается с нас самих. Каждый должен помнить прежде всего о защите своей личной информации и таким образом мы предлагаем принципы борьбы с киберпреступностью [4,5]:

1. Установить сложные пароли не только в социальные сети, но и на всю систему компьютера. Установить ативирусные и антишпионские программы.

2. Тщательно контролировать своё поведение в сетях. Не доверять, не говорить личные данные. Оградить доступ в интернет детям до 16 лет.

3. Не используйте дебетовые карты онлайн. Несанкционированные платежи дебетовой карты изымаются непосредственно с вашего банковского счёта, и даже если вы немедленно сообщите о нарушении, на восстановление прежнего баланса потребуется не одна неделя. В случае с кредитной картой в аналогичной ситуации при оспаривании подозрительных оплат клиент имеет доступ к своим счетам. Оба вида карт имеют функции оповещения либо на электронную почту или в виде СМС-текста, что даёт возможность быстрого прерывания несанкционированных действий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Глава 28 УК РФ. Электронный ресурс. URL: http://base.garant.ru/10108000/
2. Преступления в сфере информационных технологий. Материал из Википедии. Электронный ресурс. URL: https://ru.wikipedia.org/wiki/Категория:Киберпреступность
3. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / В.Б. Вехов; Под ред. акад. Б.П. Смагоринского. – М.: Право и закон, 2014.
4. Ахтырская Н. Организованная преступность в сфере информационных технологий / Н. Ахтырская // Компьютерная преступность и кибертерроризм. Исследования, аналитика. Вып. 1. – Запорожье, 2014.
5. Флюстунова А.А., Фоменко А.И. Понятие и виды преступлений в сфере высоких технологий в зарубежном уголовном законодательстве // Интеллектуальные ресурсы - региональному развитию. – 2015. – № 5. – С. 208-212.
6. Храмов В.В., Садовов В.В., Трубников А.Н., Губарев О.К. Защита информации в вычислительных системах: Учебное пособие для вузов. – Москва, 2002. – URL: https://elibrary.ru/item.asp?id=32762286 (Дата обращения 10.03.2019).