Кибербезопасность

Насыпова Л.К.

Интернет (англ.) - всемирная система объединенных компьютеров для хранения и передачи информации. Часто упоминается как **Всемирная сеть** и **Глобальная сеть**, а также просто **Сеть**.

Киберпространство (cyberspace) – это воображаемое пространство возможностей, создаваемое компьютерными системами, в частности Интернетом.

Кибербезопасность (cybersafety) – это состояние защищенности киберпространства;

Услуги Интернет

- Веб-страницы на веб-серверах. Поиск информации с помощью: *Yandex, Google, Rambler* и др.
- Файловые архивы: *DC, Torrent, Rapid* и др.
- Электронная почта
- Блог
- Веб-форум
- Чат
- Социальные сети.

Основные источники киберпреступлений

по данным Роскомнадзор

- принятие субъектом пользовательских соглашений по умолчанию
- использование "серых" мобильных приложений
- фишинг
- передача персональных данных по незащищенным каналам связи;
- использование геолокационных сервисов
- распространение своих персональных данных в открытых источниках;
- общение с незнакомыми людьми в соцсетях и др.

Фишинг

- Фишинг представляет собой сетевой вид мошенничества, при котором технически подкованные мошенники выманивают у людей конфиденциальную информацию. Это может осуществляться при помощи спама, почтовых и мгновенных сообщений, вредоносных интернет-сайтов.

- Главная задача фишинга — получение логина и пароля пользователя для определённого сайта, с дальнейшим их использованием. Это могут быть идентификационные данные вашего банковского кабинета или ПИН-код с номером карточки для вывода на свой счёт ваших денег. Часто фишинг используют для доступа к аккаунтам в соцсетях. В любом случае, когда ваш логин и пароль становятся известны жуликам, последствия для вас будут весьма удручающие.

Как защититься от фишинга

- Для защиты от фишеров следует учитывать следующие моменты:
- Помните, что пароль – только ваш, ни одна организация не станет требовать его от вас. Он необходим только для доступа к определённому сервису и только вы должны знать его.
- Внимательно проверяйте каждое полученное почтовое сообщение с неизвестного адреса на предмет наличия всевозможных просьб перейти по ссылке.
- Всегда проверяйте с помощью адресной строки, на том ли сайте вы вводите свои идентификационные данные. Обычно подделывается и домен, поэтому он бывает похожим на свой оригинал. Различие может заключаться лишь в одной букве (например, mail.ru легко превращается в meil.ru).

- Используйте последние версии интернет-браузеров и лицензионные антивирусные программы.
- При входе на банковские сайты следите за тем, чтобы было установлено защищённое соединение https.
- Если вы подозреваете, что подверглись атаке фишеров, то сразу же поменяйте пароль своего аккаунта. После этого обратитесь в службу безопасности компании, данные от которой получили мошенники.
- Во всемирной паутине развелось огромное число вирусов и хакеров, поэтому безопасность компьютера играет очень важную роль.

Социальные сети

- Информация о вас может повлиять сейчас и в будущем (репутация, работодатель).
- Вы можете заинтересовать не только кибер, но и других преступников (воры).
- Можно спровоцировать травлю себя со стороны пользователей сети.

Что делать?

- Ограничить список друзей.
- Не указывать пароли, телефон, адрес, дату рождения.
- Репутация.
- Настройки конфиденциальности аккаунта (только друзья или др.).
- Запросы в друзья только тех, кого знаете.
- Не размещать фото и видео с друзьями без их разрешения.
- Не открывать подозрительные ссылки.

Безопасность в публичных сетях

- Не передавать личную информацию через общедоступные сети WI-FI сети.
- Обновлять антивирус и брандмауэр.
- При использовании WI-FI отключить функцию **«Общий доступ к файлам и принтерам».**
- В мобильном телефоне отключить **«Подключение к WI-FI автоматически».**

Защита беспроводной сети и маршрутизатора

- Не используйте пароль, установленный по умолчанию
- Не разрешайте беспроводному устройству сообщать о своем присутствии
  Отключите вещание сетевого имени (SSID)
- Измените SSID устройства
- Шифруйте данные
  WPA-шифрование, WEP-шифрование.
- Обязательно установите надежный антивирус на всех компьютерах и устройствах.

Уголовный кодекс РФ

- **Статья 282.** Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства
  - штраф 300 000 – 500 000 рублей или в размере заработной платы или иного дохода осужденного за период от 2 до 3 лет, либо принудительными работами на срок от 1 года до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет, либо лишением свободы на срок от 2 до 5 лет.
- **Статья 242.** Незаконные изготовление и оборот порнографических материалов или предметов.
  - лишение свободы на срок от 2 до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 10 лет либо без такового.

- **Статья 280**. Публичные призывы к осуществлению экстремистской деятельности
  - штраф в размере от 100 000 - 300 000 рублей или в размере заработной платы или иного дохода осужденного за период от 1 года до 2 лет, либо принудительными работами на срок до 3 лет, либо арестом на срок от 4 до 6 месяцев, либо лишением свободы на срок до 4 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на тот же срок.
  - Те же деяния, совершенные с использованием средств массовой информации либо информационно-телекоммуникационных сетей, в том числе сети "Интернет", -
  - наказываются принудительными работами на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет или без такового либо лишением свободы на срок до 5 лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до 3 лет.

Источники

- https://lenta.ru/news/2017/11/29/kiber/
- https://habrahabr.ru/company/panda/blog/328324/
- http://www.garant.ru/article/520694/
- http://www.garant.ru/article/1095177/
- http://partnerkis.ru/kiberprostranstva/