Киберпреступность

Проект учеников 10 класса
Фаррахова Роберта, Антонова Глеба
Руководитель проекта:
Ямалетдинова Эльмира Зямиловна

Цель, задачи, актуальность

- Цель: рассказать о видах киберпреступлений и дать рекомендации по противостоянию им.

Задачи:

1. Рассмотреть виды киберпреступлений и узнать о них больше
2. Дать рекомендации по противостоянию киберпреступления

- Актуальность:

Особую актуальность проблема киберпреступности приобрела в наше время. Социологические опросы в разных странах, и в первую очередь в высокоразвитых, показывают, что киберпреступность занимает одно из главных мест среди тех проблем, которые тревожат людей.

Содержание

Введение

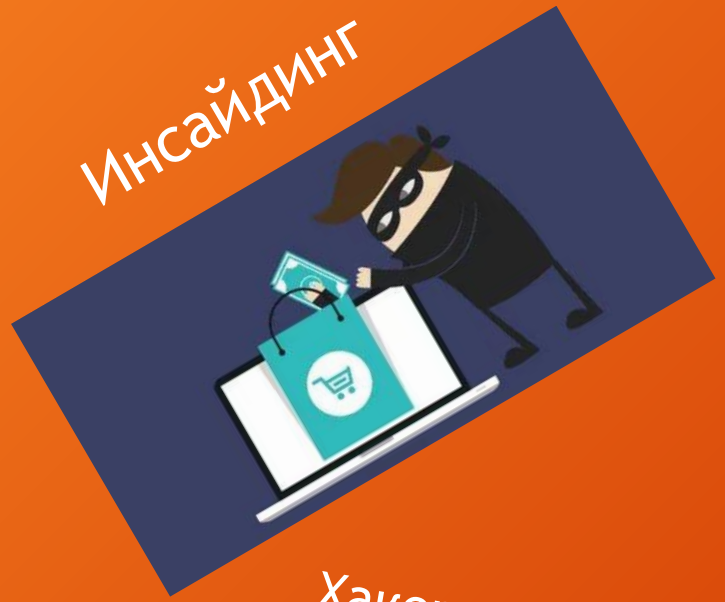
Выбранная нами тема интересна своей актуальностью. В наше время, в век информации, СМИ и интернета, эта тема как нельзя кстати. Мы узнаем какие бывают виды информационных преступлений, узнаем какие последствия ждут злоумышленников за совершенные хакерские преступления и после чего расскажем вам, как защититься, тем самым предотвратить ущерб.

Понятие “киберпреступность”

Киберпреступление - это преступная деятельность, целью которой является неправомерное использование компьютера, компьютерной сети или сетевого устройства. Киберпреступная деятельность осуществляется отдельными лицами или организациями. Некоторые киберпреступники объединяются в организованные группы, используют передовые методы и обладают высокой технической квалификацией. Другие – начинающие хакеры.

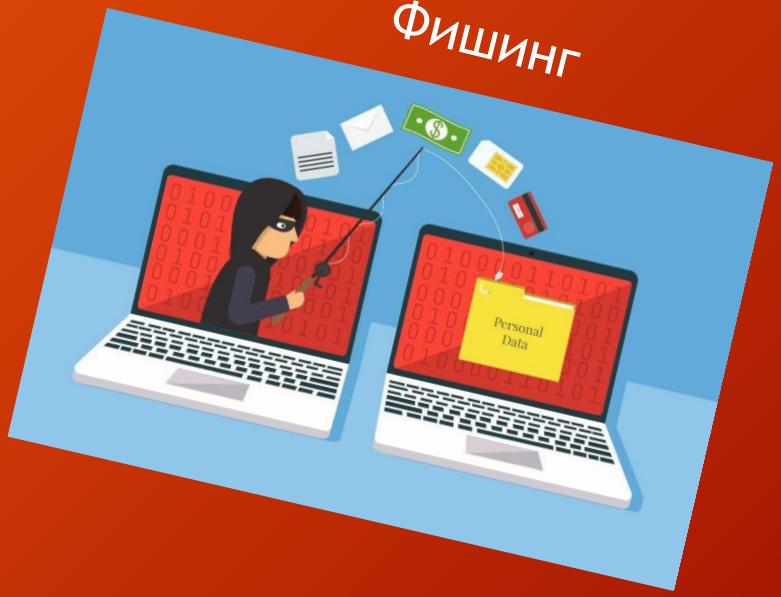
Примеры киберпреступлений

Инсайдинг



В ходе исследования мы выделили несколько основных видов киберпреступлений. Среди них: Фишинг, Инсайдинг, Хакерство, Кибersквоттинг , Похищение цифровой личности, Телекоммуникационные преступления.

Фишинг



Хакерство

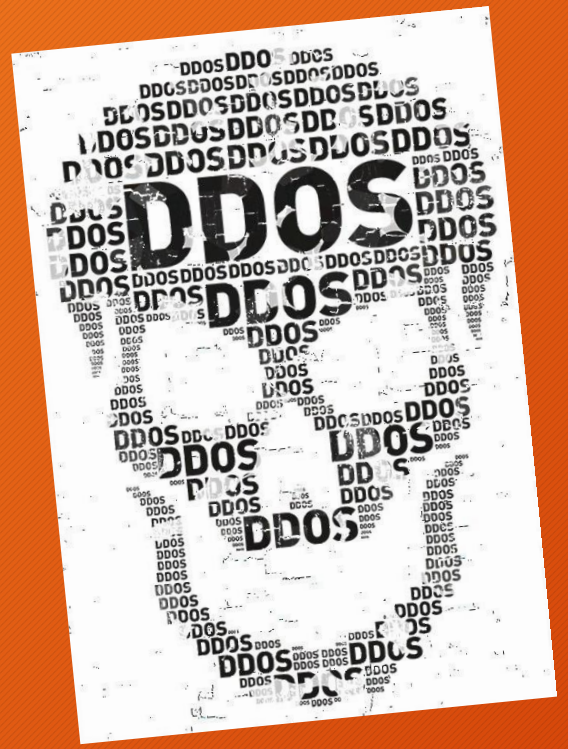
Похищение цифровой личности

Кибersквоттинг

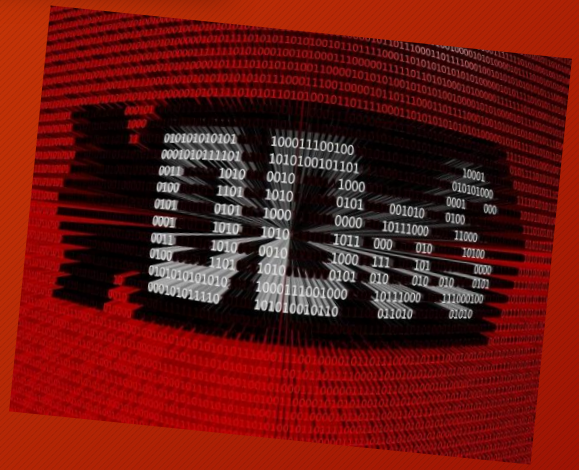
Рекомендации по защите от мошенников в интернете

1. Использование антивирусных программ.
2. Использование сложных уникальных паролей для каждой службы.
3. Регулярное обновление программного обеспечения.
4. Ограничение личной информации в соцсетях
5. Не подключайтесь к сомнительному WiFi.
6. Не подключайте чужие USB-носители.
7. Проверяйте аккаунт пользователя, прежде чем добавлять его в друзья.
8. Никогда не открывайте письма на электронной почте, если не уверены в отправителе.
9. Не нажимайте на кнопки, ссылки и баннеры, если не знаете, на какой ресурс они ведут.
10. Используйте проверенные VPN сервисы

DDoS-атаки



Заголовки новостей сегодня пестрят сообщениями о DDoS-атаках. DDoS (Distributed Denial of Service) атаки - это хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён. Распределенным атакам «отказ в обслуживании» подвержены любые организации, присутствующие в интернете. Вопрос не в том, атакуют вас, или нет, а в том, когда это случится. Государственные учреждения, сайты СМИ и электронной коммерции, сайты компаний, коммерческих и некоммерческих организаций – все они являются потенциальными целями DDoS-атак.



VPN-сервисы

Каждый конкретный VPN — это виртуальная частная сеть. Она представляет собой что-то вроде объездной дороги, которая, как и основная, дает возможность добраться из той же точки «А» в ту же точку «Б», но предоставляет массу дополнительных нюансов. К примеру, если правительство перекрыло основную дорогу к конкретному сайту, по этой самой объездной к нему все еще можно добраться. Более того, ездить по ней порой бывает заметно дешевле.

Опрос

Вопросы	Учителя	Родители	Учащиеся школы
Что такое киберпреступность?	21	19	30
Кто такие хакеры, фишеры, инсайдеры?	15	11	24
Какие виды киберпреступности существуют?	12	8	22
Предусматривает ли закон РК наказание за киберпреступления?	26	20	30

Мы провели опрос среди родителей, учеников и учителей нашей школы. Результаты опроса вы можете увидеть в данной таблице. Благодаря опросу мы на личном опыте убедились, что юное поколение более осведомлено на данную тему.

Вывод

- Таким образом, можно считать, что поставленные цели достигнуты. Мы узнали много нового, интересного и полезного. Полученные знания пригодятся в жизни всем нам.
  Чем сильнее становится зависимость жизни общества от компьютерных систем, тем опаснее уязвимость России и других стран от всевозможных мастей киберпреступников. О безопасности надо думать сегодня, завтра уже может быть поздно.

Литература

- https://infourok.ru/issledovatelskaya-rabota-po-teme-kiberprestupnost-3249489.html
- https://ru.wikipedia.org/wiki/Фишинг
- https://ru.wikipedia.org/wiki/Кибersквоттинг
- https://rusmonitor.com/13-prostykh-pravil-kotorye-pomogut-vam-ne-stat-zhertvoj-kiberprestupleniya.html
- https://obuchonok.ru/node/7648
- https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime
- http://elcomrevue.ru/kibeoprestupnost-chto-eto/
- https://infourok.ru/proekt-po-informatike-kiberprestupnost-2973910.html
- https://ru.vpnmentor.com/blog/плюсы-и-минусы-vpn-сервисов/
- https://androidinsider.ru/obzory-prilozhenij/5-prichin-ne-polzovatsya-vpn.html
- https://habr.com/ru/company/ruvds/blog/321992/