# МБОУ-лицей 21 им. А.П. Ермолова

## Проект: «Киберпреступность»

АВТОР: Давыдов Ф.М.
Руководитель: Грачева С.А.

Начало работы: май 2018г.
Конец работы: май 2020г.

Орел, 2020г.

# Содержание.

# Введение.

Мы живем в 21 веке, в век информационных технологий. Почти у каждого из нас есть компьютер, телефон, плеер, телевизор. Более 70% процентов населения земли не могут представить свою жизнь без электронных технологий. Сегодня компьютеры используются во всех сферах жизнедеятельности человека – от повседневного быта до государственной безопасности. Быстрое увеличение персональных компьютеров и быстро развивающийся рынок новых электронных устройств изменили и способы проведения досуга, и методы ведения бизнеса.

Мы храним огромные объемы информации в компьютерах и часто хотим эту информацию скрыть. Сегодня, как никогда ранее, актуальна проблема защиты личных и конфиденциальных данных. По мере роста развития информационных технологий и развития систем безопасности, растет и количество киберпреступлений. Невозможно создать идеальную систему безопасности. В любой системе есть уязвимость.

**Цель работы:**

- изучить проблемы развития киберпреступности в мире и России и найти
способы ее профилактики.

**Задачи:**

1. Изучить понятие киберпреступность.
2. Рассмотреть виды киберпреступлений.
3. Провести опрос в социальных сетях.
4. Найти примеры киберпреступлений в мире, России.
5. Дать рекомендации противостояния хакерам в домашних условиях.

**Объект исследования:** киберпреступления.

**Гипотеза:**

Киберпреступность может перерасти в более глобальную проблему и стать
серьёзней бытовых преступлений

## Актуальность

Выбранная мной тема интересна своей актуальностью. В наше время, в век информации, СМИ и интернета, эта тема как нельзя кстати. Смотря фильмы, сериалы, передачи, мы задались вопросом, а все ли так, как показано на экране? Все ли настолько плохо или настолько хорошо? Стоит ли бояться киберпреступлений нам - обычным людям? И если да, то как от них уберечься, защититься?

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.

Предмет исследования: поиск методов профилактики и борьбы с киберпреступлениями.

Проблема: отсутствие у людей пожилого возраста представления о киберпреступности.

# Что такое киберпреступность?

**Киберпреступность** – это преступления, совершаемые в сфере информационных технологий, так называемом виртуальном пространстве.

**Можно выделить основные виды киберпрестсупности:**

1.кража паролей,

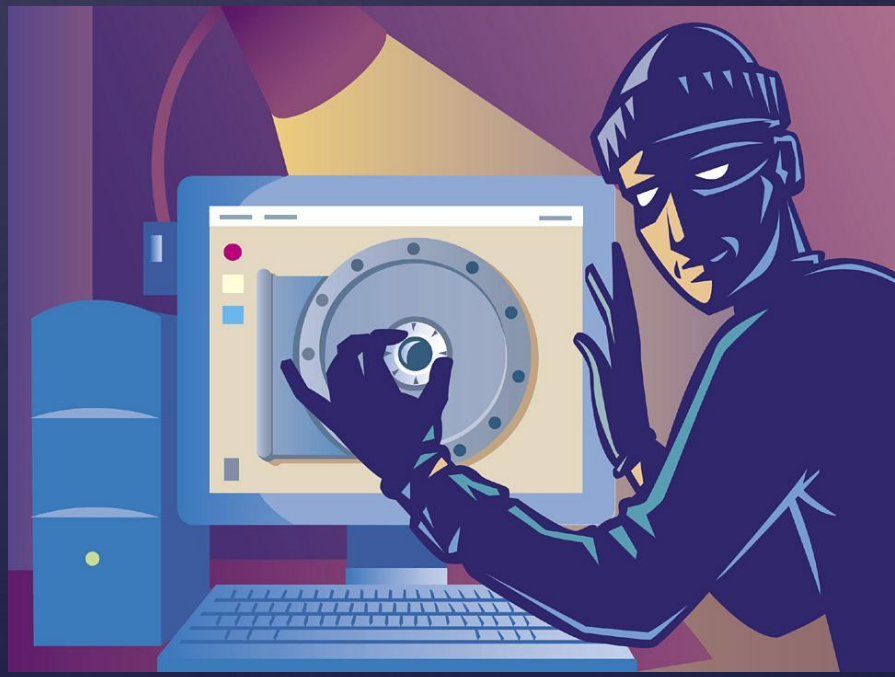
2.номеров кредитных карт,

3.распространение вирусных программ; 4. распространение оскорбляющей и абсурд информации в сети Интернет.

# Фишинг.

Это один из способов интернет-мошенничества, когда всеми возможными правдами и неправдами у вас пытаются узнать различные персональные данные (пароли, логины, номера банковских карт и счетов). Смысл заключается в том, чтобы побудить вас перейти по фишинговый ссылке на поддельную страницу, визуально похожую на настоящую, например, банка, где под различными

предлогами выудить персональную информацию.



# Спам.

# Хакерство.

**Спам** — массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получать. Распространителей спама называют спамерами.

**Хакер** - чрезвычайно квалифицированный IT-специалист, человек, который понимает самые глубины работы компьютерных систем.

# Похищение цифровой личности.

## Телекоммуникационные преступления:

- Роумерское мошенничество
- Хищение трафика
- Незаконное оказание услуг электросвязи.

# Примеры киберпреступлений в мире и России.

Интернет уже не тот, что был несколько лет назад. Сейчас в интернете больше сервисов, информации и возможностей.
Киберпреступники тоже очень быстро развиваются, они становятся умнее, опытнее и профессиональнее. Но лишь сейчас начали уделять особое внимание этой угрозе. Если раньше вопрос о безопасности в Интернете сводился к защите личных данных, то теперь необходимо думать о защите от незаконного проникновения на секретные базы данных и целые компьютерные системы.

# Уголовно-правовые меры по борьбе с киберпреступностью.

Главные проблемы преступлений в сфереинформационных технологий – это слабая подготовка правоохранительных органов по борьбе с киберпреступностью и расследованию преступлений в сфере информационных технологий, а также высоким уровнем скрытности преступлений в этой сфере. Поэтому, только 15% от общего числа киберпреступлений доходят до правоохранительных органов и становятся известными общественности.

В России борьбой с киберпреступностью занимается Управление «К» МВД РФ. Управление «К» - одно из самых засекреченных подразделений МВД РФ, а также входит в Бюро СТМ МВД РФ.

# Опрос респондентов в социальных сетях и лично.

По результатам 94% опрошенных знают, что такое киберпреступность, и те же 94% сталкивались с ней в интернете. Самыми распространёнными видами, судя по результатам опроса, являются спамерство и хакерство. Так респондентам был задан вопрос: «Какие пути решения проблемы киберпреступности Вы видите?», на что получили следующие ответы:

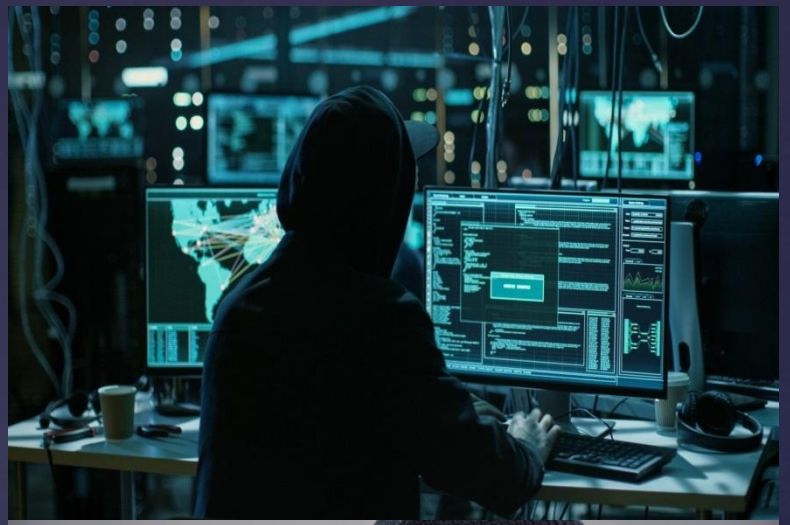
- устанавливать длинные пароли;
- делать регулярные обновления программного обеспечения на компьютерах и смартфонах;
- пользоваться антивирусными программами;
- не сообщать личные данные сомнительным людям, сайтам, в ответ на телефонные звонки от неизвестных абонентов;

**Памятки противостояния хакерам в домашних условиях:**

1. Регулярно скачивайте обновления для программного обеспечения часть атак идёт через неисправленные ошибки.
2. Настройте межсетевой экран для фильтрации нежелательных входящих соединений.
3. Установите качественное антивирусное и антишпионское программное обеспечение.
4. Установите спам-фильтр в почтовые программы (например, в Outlook) Не открывайте писем от пользователей, которых вы не знаете.
5. Не переходите по ссылкам на известные сайты (соц.сети, банки, интернет-магазины) непосредственно из писем. Очень часто такие письма являются фишинговыми. Часто посещаемые сайты лучше держать в браузере в закладках. Ну или каждый раз искать эти сайты в яндексе, гугле.
6. Придумывайте (возможно, с помощью специальных генераторов) надёжные не повторяющиеся пароли.
7. Храните несколько резервных копий важных данных.
8. Обращайте внимание, если ваши знакомые начинают вести себя необычно игнорируйте их просьбы одолжить денег или предоставить другие ресурсы. Лучше уточнить подробности по телефону или лично.

# Заключение.

К вопросу о киберпреступности нужно отнестись очень серьезно. Технологии в современном мире не стоят на месте и быстро развиваются, что дает новые возможности для совершения нового рода киберпреступлений. Правительственным органам нужно довольно серьезно заняться решением проблемы киберпреступности, иначе это может привести к необратимым последствиям.



# Источники информации.


- . Киберперступность: http://www.securitylab.ru/news/tags/%EA%E8%E1%E5%F0%EF%F0%E5%F1%F2%F3%EF%ED%EE%F1%F2%FC/
- 2. Википедия. Преступления в сфере информационных технологий: https://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных_технологий
- 3.Википедия. Фишинг: https://ru.wikipedia.org/wiki/Фишинг
- 4. Татьяна Тропина <<Киберпреступность и кибертерроризм>>: http://www.phreaking.ru/showpage.php?pageid=542335. И. М. РАССОЛОВ <<Киберпреступность: понятие, основные черты, формы проявления>>: http://www.center-bereg.ru/h1529.html
- 6. Компьютерные вирусы : http://dic.academic.ru/dic.nsf/ruwiki/977057
- 7. Фишишнговая атака: http://it-web-log.ru/2012/02/fishingovaya-ataka/
- 8. Deep Web – глубинный интернет. Тёмная материя, обратная сторона Интернета: http://banda-rpt.com/publ/1/1/13-1-0-1718
- 9. Уголовный кодекс РФ: http://www.zakonrf.info/uk/gl28/
- 10. Управление <<К>>: https://ru.wikipedia.org/wiki/Управление_«К»
- 11. Убытки от киберпреступности: http://www.rg.ru/2013/10/16/spam.html
- 12. Norton Cybercrime Report: http://us.norton.com/cybercrimer
- 13. Телекоммуникационны технологии: http://book.itep.ru