**МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ
ОБЩЕОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ГОРОДСКОГО ОКРУГА БАЛАШИХА
«ГИМНАЗИЯ №2»**

# ПРОЕКТ

на тему «Киберпреступность»

Королева Кирилла Ивановича,
ученика 9 «А» класса
**Руководитель проекта:**
Терехова Елена Дмитриевна
учитель информатики

2019 г

## Оглавление

# Глава 1

## 1.1.ВВЕДЕНИЕ:

В современном мире невозможно обойтись без интернета. По существу, Интернет представляет собой глобальную сеть, используемую для связи и обмена данными, также здесь существует свой вид преступности.

Что такое преступление?

Все мы знаем что преступление – это любое криминальное действие, совершение которого влечёт применение к лицу мер уголовной ответственности.

В современном мире человеческая деятельность все больше смещается в виртуальную реальность – Интернет. Интернет и представляет собой глобальную сеть, используемую для связи и обмена дынными. Кроме этого, в сети происходит большое кол – во различных сделок, например: покупка, совершённая человеком в интернет-магазине, или оплата сотовой связи, или заказ пиццы и т.д.

Но всегда ли все происходит честным путём?

Я решил разобраться так ли всё гладко в интернете. Существуют ли киберпреступники, какие виды преступлений в сети бывают. Каково наказание в случае в случае поимки.

## Цель и задачи проекта

**Цель**

Узнать какие существуют способы профилактики киберпреступности и борьбы с ней, провести опрос в социальных сетях на тему .

**Задачи:**

1. Дать определение киберпреступности и рассказать о её видах.
2. Рассказать о правилах безопасности в интернете, а также о способах борьбы с киберпреступностью.
3. Провести опрос в социальной сети вконтакте среди моего класса.
4. Сделать вывод относительно результатов опроса и дать рекомендации.

### 1.2.Ход работы:

В интернете я нашел множество статей на эту тему и выделил из них основную часть. И понял что существует 8 групп киберпреступлений. Все они отличаются между собой. Я дал определение каждой из групп и рассказал о правилах безопасности в интернете. Потом я провел опрос среди своего класса и оказалось что 58% подвергались заражению их устройств вирусами, а 22% становились жертвой кражи материальных средств за счет вирусов. Я сделал вывод что мой проект актуален и всем будет полезно еще раз ознакомится с правилами безопасности в сети интернет. Также я дал рекомендации по поводу установки антивируса и предложил бесплатную версию для мобильных устройств.

### 1.3.Теоретический материал:

Я выяснил что **киберпреступность** - преступления, совершаемые в сфере информационных технологий. Существует ряд типов подобных киберпреступлений, задачей которых является похищение личной конфиденциальной информации. Хотя в некоторых случаях правонарушителями движет более серьезная мотивация (например, материальная или связанная с изменение политических настроений), большая часть внимания сосредоточена на обхо-

де законов и поиске уязвимостей в технологиях, которые защищают персональные конфиденциальные сведения.

**Существуют разные нарушения. Их можно разделить на 8 групп:**

**1) Нарушение авторского права**

Правонарушение, суть которого составляет использование произведений науки, литературы и искусства, охраняемых авторским правом, без разрешения авторов или правообладателей или с нарушением условий договора об использовании таких произведений. К числу основных способов нарушения авторских прав относится незаконное копирование и распространение произведения, а также плагиат.

**2) Спам**

Массовая рассылка корреспонденции рекламного характера лицам, не выражавшим желания её получать.

**3) Социальные и политически мотивированные киберпреступления**

Некоторые типы киберпреступлений направлены на изменения настроений в политической среде или нанесение намеренного вреда или снижения влияния отдельных личностей или группы людей.

**4) Преступления на почве ненависти и домогательства**

Преступления на почте ненависти по отношению к личности или группе людей обычно совершаются на основе гендерной, расовой, религиозной, национальной принадлежности сексуальной ориентации и других признаков. Примеры: домогательства и рассылка оскорбительных сообщений и вброс ложных новостей, касающихся определенной группы лиц.

Анонимность и легкодоступность интернета серьезно затрудняют борьбу с преступлениями на почве ненависти.

**5) Терроризм**

Комплекс незаконных действий, создающих угрозу государственной безопасности, личности и обществу. Может привести к порче материальных объектов, искажению информации или другим проблемам. Основной целью

кибертерроризма является получение преимущества в решении социальных, экономических и политических задачах.

**6) Кибербуллинг**

Интернет-травля или Кибертравля - намеренные оскорбления, угрозы, диффамации и сообщение другим компрометирующих данных с помощью современных средств коммуникации, как правило, в течение продолжительного периода времени. Киберпреступления, связанные с недозволенными действиями.

«dark web» - изнанка интернета (или глубокий интернет), используется с целью совершения противозаконных деяний.

**7) Груминг**

Тактический подход взрослого человека к несовершеннолетнему, как правило, с сексуальными целями. Речь идет о намеках, соблазнениях и манипуляциях, то есть уголовно наказуемых действиях. Распространение наркотиков и оружия.

**8) Шпионаж**

Хакеры распространяют вирусы в сети. Вирусы - попав однажды в ваш компьютер/планшет/смартфон, могут тихо собирать и переправлять вашу личную информацию и переписку, отслеживать перемещения телефона, включать микрофон и видеокамеру и многое другое.

## Глава 2

### 2.1. Правила безопасности в интернете и способы борьбы с киберпреступностью

1.Используйте лицензионное программное обеспечение для защиты от заражения компьютера или мобильного устройства при установке различных программ;

2.Установите антивирусную программу не только на персональный компьютер, но и на смартфон, планшет и другую технику;

3.Не загружайте файлы из непроверенных источников;

4.Не переходите по ссылкам, содержащимся в спаме и других подозрительных электронных письмах отправителей, которых вы не знаете;

5.Не сообщайте никому свои пароли и личные данные;

6.Откажитесь от покупок на малоизвестных и подозрительных интернет-сайтах и у лиц, осуществляющих продажу товаров или услуг в социальных сетях, особенно при необходимости внесения полной предоплаты за товар или услуги;

7.Используйте сложные пароли, состоящие из комбинаций цифр и букв или иных символов;

8.Воздержитесь от паролей – дат рождения, имен, фамилий, то есть тех, которые легко вычислить либо подобрать.

Как уже отмечалось, киберпреступность не признает границ и не ограничивается рамками одного государства, а, следовательно, эффективное противодействие ей возможно только на уровне международного сотрудничества.

### 2.2. Борьба с киберпреступностью

Разработка национальных систем борьбы с данным видом преступности, безусловно, необходима, но локальное расследование киберпреступлений усложняется по нескольким причинам:

- требуется специфическое образование и опыт;
- часто преступник и жертва находятся в разных странах, а следственные действия правоохранительных органов как раз ограничены пределами одного государства;
- преступники имеют возможность выбрать наиболее лояльную правовую систему.

Говоря о России, стоит отметить, что в нашей стране с 1992 года существует Бюро специальных технических мероприятий МВД России.

Сотрудники Бюро, проходят специальную подготовку в лучших технических ВУЗах страны, а также в учебных центрах крупнейших компаний, работающих в IT-отрасли.

# Глава 3

## 3.1. Результаты опроса среди класса:

Я провел опрос среди своего класса и получил такие результаты: 58% учеников подвергались заражению их устройств вирусами(См.Приложение 1). Также 22% учеников подвергались краже финансовых средств последством заражения вирусом(См.Приложение 2).

## 3.2. Вывод:

По результатам данного тестирования видно, что эта тема актуальна, так как большая часть моего класса уже подвергались заражению устройства вирусами. И для них будет полезно ознакомиться с правилами безопасности в интернете.

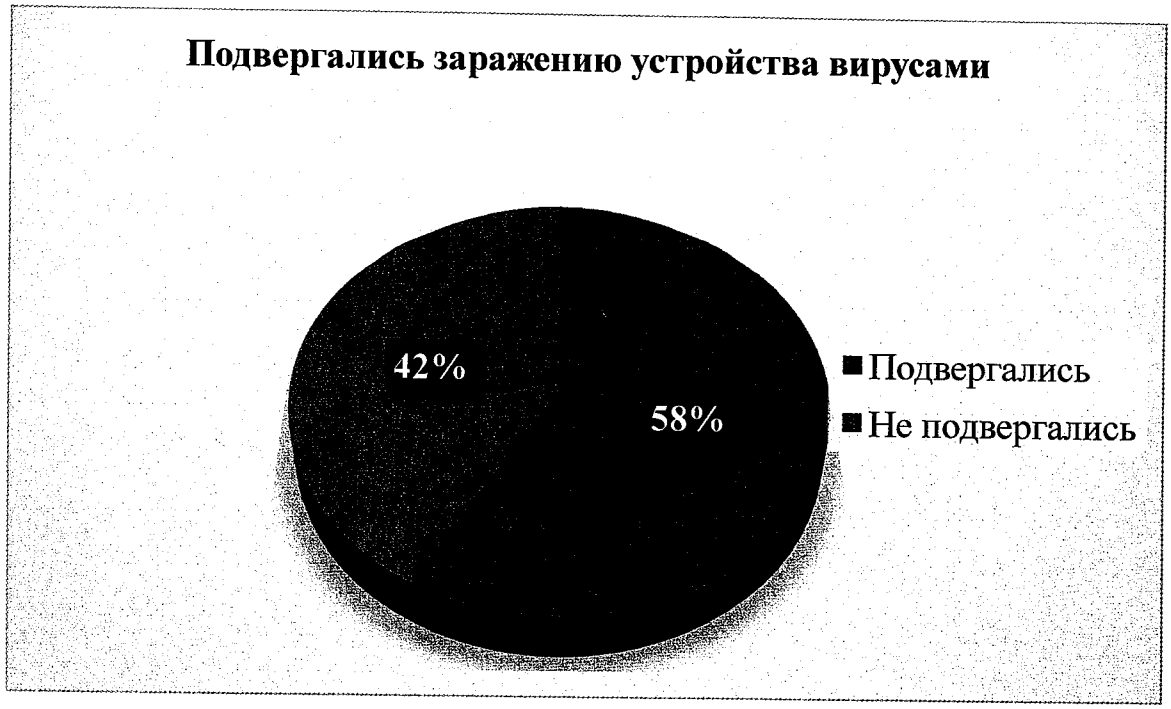
## 3.3. Рекомендации:

Я бы хотел предложить владельцам смартфонов на операционной системе Android установить бесплатный антивирус Avast Mobile Security.

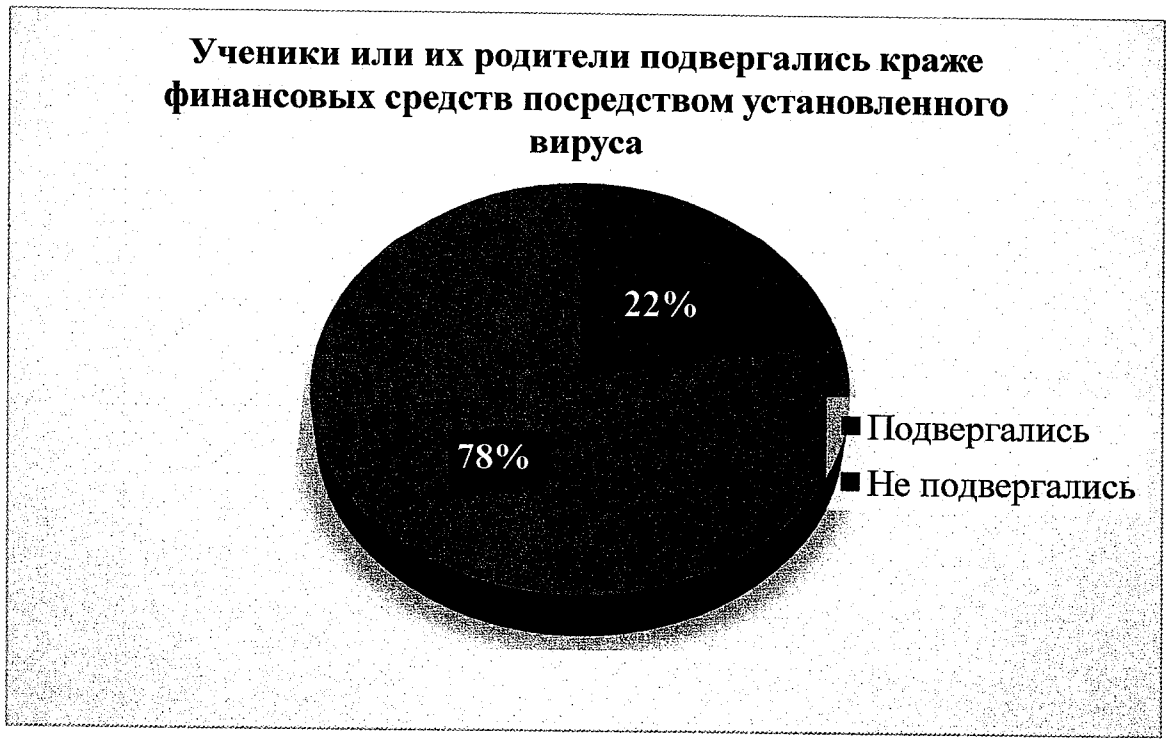
Вы можете скачать его через поисковую строку магазина приложений Play Market, введя в поисковую строку Avast Mobile Security и нажав кнопку установить, или отсканировать этот QR код, перейти на сайт и нажать кнопку установить.

### 3.4.Список литературы:


1. Тропина Т.Л. Интернет и терроризм: прежние цели - новые средства, 2005
2. studwood.ru/1658101/informatika/kiberprestupenost_problemy_puti_reshen iya
3. https://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных_т ехнологий
4. https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html
5. https://sledcomrf.ru/news/311007-profilaktika-kiberprestupleniy.html
6. https://urist.one/dolzhnostnye-prestupleniya/kiberprestupnost/kiberprestuplenie.html




**Приложение 2**


Ученики или их родители подвергались краже финансовых средств посредством установленного вируса
22%
78%
Подвергались
Не подвергались