


Презентация на тему “Кибербезопасность”

Подготовил: Голубев Рустам
Руководитель: Стопина Ольга Александровна



Проблема. В современном мире бурно развиваются технологии обработки, хранения и передачи информации. Применение информационных технологий требует повышенного внимания к вопросам кибербезопасности. Уничтожение информационных ресурсов, их недоступность или несанкционированное использование вследствие нарушений информационной безопасности, вызывают серьезные проблемы у граждан. Население не относится к безопасности в интернете с серьёзностью, что позволяет злоумышленникам свободно заниматься преступностью в интернете.

Актуальность. С нынешними тенденциями можно с уверенностью сказать, что безопасность в интернете является актуальной темой, так как пользователей интернета становится больше, а преступность в сети не стоит на месте.

Цель. Изучить вопросы кибербезопасности и разработать рекомендации по безопасному пользованию интернетом

Задачи.

- Объяснить, что такое кибербезопасность.
- Рассказать о самых распространенных видах мошенничества..
- Рассказать о мерах предосторожности в интернете.
- Провести опрос по данной теме среди подростков.
- Разработать правила безопасного пользования интернетом.



Теоретическая часть

Что такое кибербезопасность?

Кибербезопасность - это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

- **Безопасность сетей** – действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ
- **Безопасность приложений** – защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.
- **Безопасность информации** – обеспечение целостности и приватности данных как во время хранения, так и при передаче.
- **Операционная безопасность** – обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.
- **Повышение осведомленности** – обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства.

Масштаб распространения киберугроз

Год за годом в мире становится все больше угроз и происходит все больше утечек данных. Статистика шокирует: согласно отчету RiskBased Security, только за первые девять месяцев 2019 года было зафиксировано 7,9 миллиардов случаев утечки данных. Эти цифры превышают показатели за тот же период 2018 года более чем в два раза (на 112 %).



Виды киберугроз



Кибербезопасность борется с тремя видами угроз:

Киберпреступление – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.

Кибератака – действия, нацеленные на сбор информации, в основном политического характера.

Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.



Угрозы, с которыми может столкнуться обычный пользователь интернета

Вирусы – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.

Трояны – вредоносные файлы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троян на свой компьютер, а потом собирают данные или повреждают их.

Шпионское ПО – программы, которые в тайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.

Программы-вымогатели – файлы, которые шифруют содержимое компьютера. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.

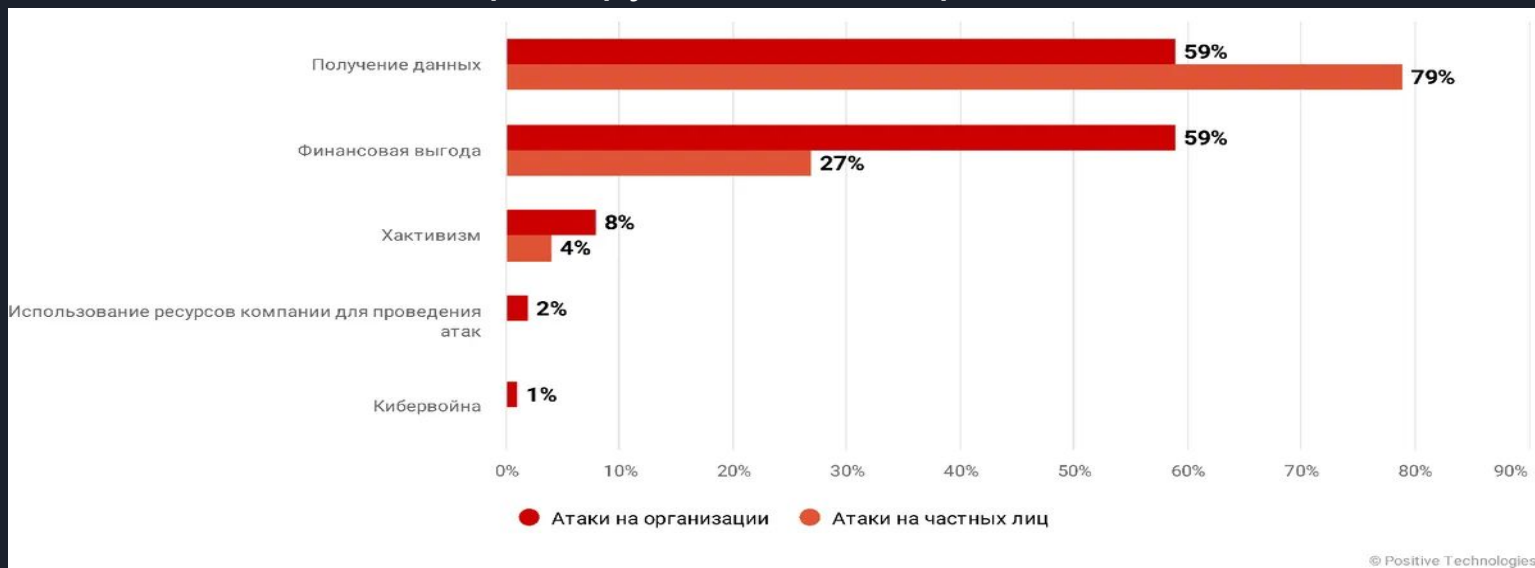
Рекламное ПО – программы рекламного характера, с помощью которых может распространяться вредоносное ПО.



Основная часть

Зачастую бывает так, что люди пренебрегают самыми базовыми правилами пользования интернетом, что в итоге порождает удручающие цифры в различных статистиках компаний, занимающихся кибербезопасностью.

Вот, к примеру, анализ кибератак за 2019 г.



О простейших методах мошенничества в интернете (например "выигрышей в лотерее или конкурсе" и вообще чего-то бесплатного) можно сказать, что тут стоит мыслить рационально - вряд ли получится так, что вы особенный, и что вам правда повезло что-то выиграть там, где, скорее всего, вы даже не участвовали. Это типичный случай фишинга.

ПАО "Унитарный
Дотационный Центр"
РФ, г. Москва, проспект
Вернадского 180
Служба поддержки граждан:
anmcontact@yahoo.com

**Социальная
Викторина**

персональное
извещение
№776828PE

**ЗДРАВСТВУЙТЕ,
ПОЗДРАВЛЯЕМ ВАС!**
**ВЫ БЫЛИ ПРИГЛАШЕНЫ НА ДАННЫЙ САЙТ, ТАК КАК ВАШИ ДАННЫЕ
СОДЕРЖАТСЯ В РЕГИОНАЛЬНОМ СОЦИАЛЬНОМ РЕЕСТРЕ.**

ВАМ ПРЕДОСТАВЛЕНА ВОЗМОЖНОСТЬ ПРИНЯТЬ УЧАСТИЕ В СОЦИАЛЬНОЙ
ВИКТОРИНЕ И ПОЛУЧИТЬ ДЕНЕЖНОЕ ВОЗНАГРАЖДЕНИЕ
МАКСИМАЛЬНО ДО 200 000 РУБЛЕЙ!
моментальным платежом
на Вашу карту или электронный кошелек.



Нажмите кнопку для участия в социальной викторине



Опрос

Я провёл опрос школьников 13-15 лет. Его суть заключалась в том, сталкивались ли они с интернет-угрозами. Были заданы такие вопросы:

Считаете ли вы себя защищенным в сети интернет?

1. Да 2. Нет 3. Скорее да, чем нет 4. Скорее нет, чем да

Пользуетесь ли вы антивирусом?

1. Да 2. Нет

Сталкивались ли вы с вредоносным ПО?

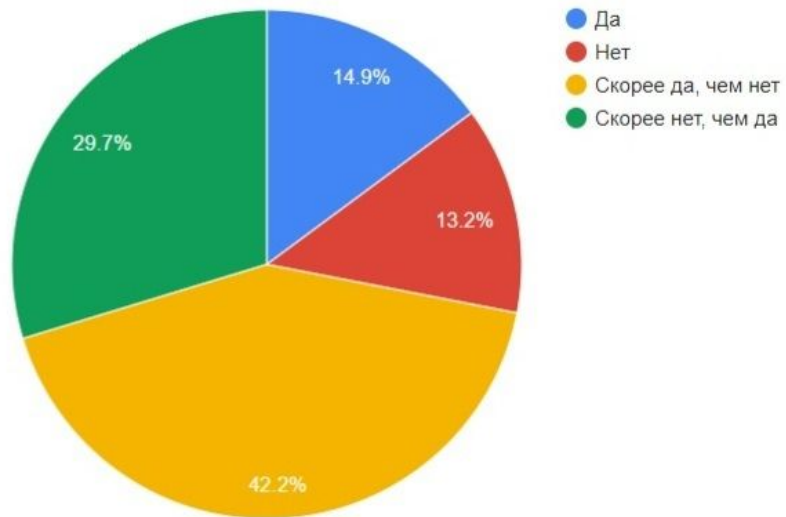
1. Да 2. Нет

Если да, выберите вид угрозы, с которой вы сталкивались чаще всего.

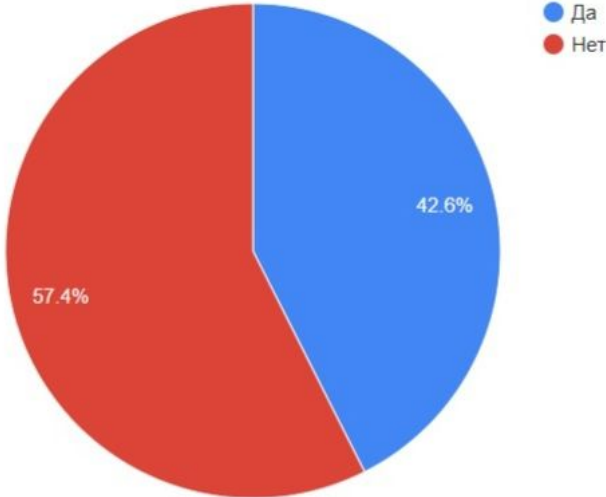
1. Вирус 2. Троян 3. Вымогатель 4. Рекламное ПО 5. Другое

Результаты получились такие

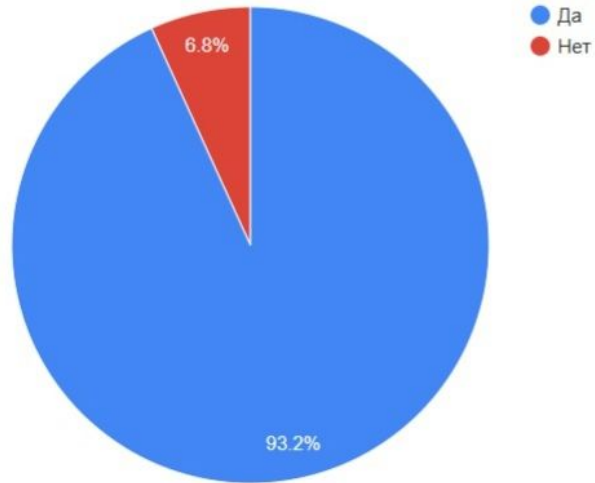
Первый вопрос



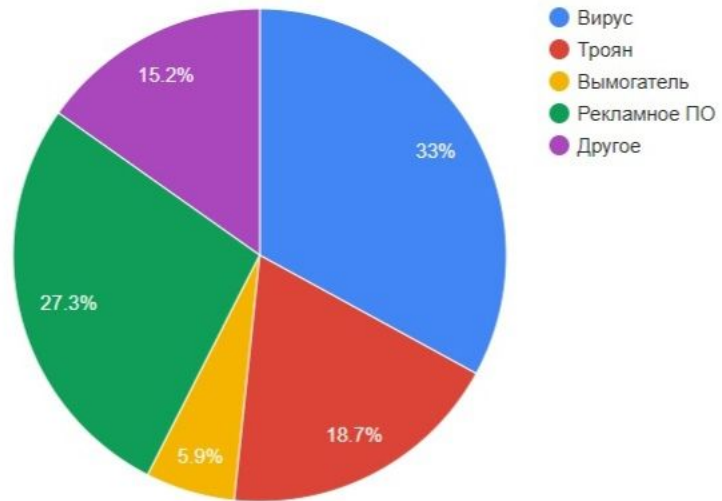
Второй вопрос




Третий вопрос



Четвёртый вопрос





Согласно результатам анкетирования (см. рис. 1) большая часть (42.2%) ребят считает себя скорее защищенными в интернете, но не до конца в этом уверены. Также 29.7% школьников чувствуют себя более незащищенными. Это говорит о том, что многие осознают серьезность безопасности в интернете.


Из рис. 2 видно, что большинство (57.4%) опрошиваемых не использует антивирус.

Из рис. 3 же можно сделать несложный вывод, что практически все респонденты (93.2%) сталкивались с вредоносным ПО.

Глядя на рис. 4, можно сделать вывод, что чаще всего респонденты встречались с такими угрозами как вирусы (33%), рекламное ПО (27.3%) и трояны (18.7%)



Заключение



Я выполнил свою цель - дал рекомендации по безопасному пользованию интернетом.

- Я объяснил, что такое кибербезопасность
- Я рассказал о самых распространенных видах мошенничества
- Я рассказал о мерах предосторожности в интернете
- Я провел опрос по данной теме среди подростков
- Я разработал правила безопасного пользования интернетом