# Проект на тему: «Безопасность в интернете»

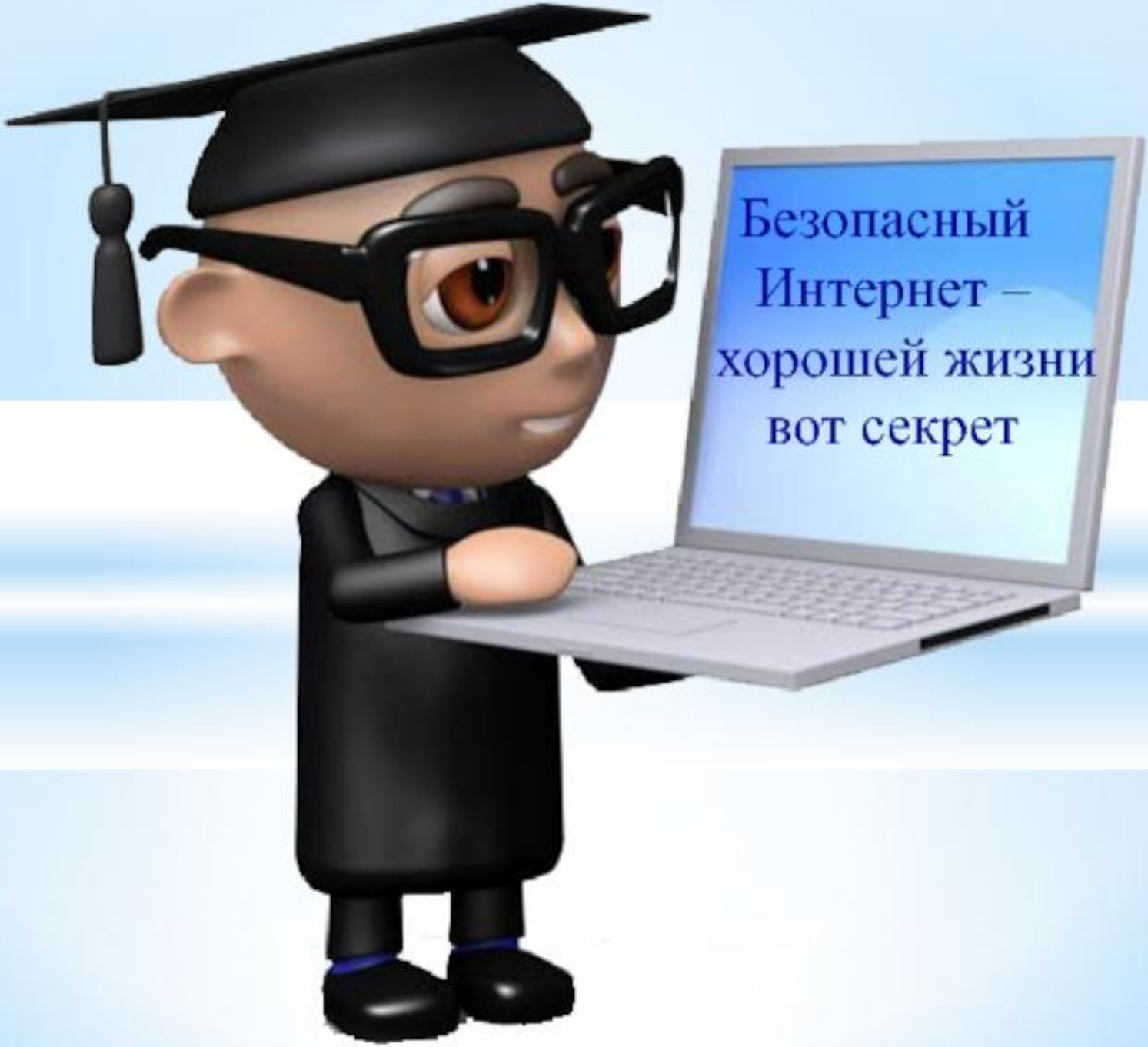
Подготовил:
Ученик 7а класса
Курышов Игорь
Наставник:
Кулакова Татьяна Валерьевна

# План

- ***1.Введение***
- ***2.Теоретическая часть:***
  - *1)Что такое интернет?*
  - *2)Чем опасен интернет?*
  - *3) Способы обезопасить себя.*
- ***4. Заключение***
- ***5. Источники***

# Введение

- **30 октября в России отмечают Всемирный день безопасности в сети Интернет.**
- С целью обеспечения информационной безопасности пользователей при использовании ресурсов сети во многих образовательных организациях проводят открытые уроки и семинары.
- Наш семинар призван привлечь дополнительное внимание преподавателей к проблеме подростковой безопасности в Интернете и развитию информационной грамотности.


Безопасный
Интернет –
хорошей жизни
вот секрет

# Что такое интернет?

- Интерне́т (англ. Internet) — это всемирная система объединённых компьютерных сетей для хранения и передачи информации.
- С появлением в 1969 г. Интернета весь мир поделился на два понятия: ОНЛАЙН (Интернет) и ОФФЛАЙН (обычная, традиционная жизнь). Практически все, что есть в ОФФЛАЙНЕ, уже присутствует и в ОНЛАЙНЕ.
- В связи с массовой популярностью сети Интернет важной проблемой сегодня является безопасность в глобальной сети. Касается данная проблема абсолютно всех, начиная от детей и заканчивая пенсионерами.

# Чем опасен интернет?

Интернет опасен различными сторонними программами, вирусами, и других различных повреждающими компьютер компонентами.

Я расскажу о некоторых вирусах.

# Стиллер (от английского *to steal*, воровать)

- Класс малварей предназначенный для кражи данных с компьютера зараженного. Вирус проникает в хранилище данных популярных программ и ворует данные логинов и паролей, отсылая их злоумышленнику.

- Что подвергается стиллу чаще всего:
  - Данные банков
  *Например: Сбербанк, Тинькофф, Киви, Вебмани, Пейпал.*
  - Аккаунты игровых платформ
  *Например: Steam, Uplay, Origin, Battle.net.*
  - Криптовалютные биржи
  *Например: Coinbase, Localbitcoins.*
  - Данные соц сетей
  *Например: VK, OK, Instagram, Youtube.*

  Список может быть абсолютно разнообразным, всё зависит от желания злоумышленника.

# Методы борьбы со стиллером

- - Не сохранять пароли в браузере, лучше всего держать их на бумажке, или же в телефоне.
  - Использовать НЕ популярные браузеры.
  - Использовать антивирусы.
  - Периодически проверять операционную систему программами типа: Hitman Pro, Malwarebytes.

# **Трояна́ вирусная программа** (также — **трояна́**)

- Разновидность вредоносной программы, проникающая в компьютер под видом легитимного программного обеспечения, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации о банковских картах, передача этой информации злоумышленнику, а также использование, удаление или злонамеренное изменение, нарушение работоспособности компьютера, использование ресурсов компьютера в целях майнинга, использование IP для нелегальной торговли.
- Троянские программы распространяются людьми — как непосредственно загружаются в компьютерные системы злоумышленниками-инсайдерами, так и побуждают пользователей загружать или запускать их на своих системах.
- Для достижения последнего троянские программы помещаются злоумышленниками на открытые или индексируемые ресурсы (файл-серверы и системы файлообмена), носители информации, присылаются с помощью служб обмена сообщениями (например, электронной почтой), попадают на компьютер через бреши безопасности или загружаются самим пользователем с адресов, полученных одним из перечисленных способов.
- Иногда использование троянов является лишь частью спланированной многоступенчатой атаки на определённые компьютеры, сети или ресурсы.

# Методы борьбы с Троянами

- В целом, троянские программы обнаруживаются и удаляются антивирусным и антишпионским ПО точно так же, как и остальные вредоносные программы.
- Троянские программы хуже обнаруживаются контекстными методами антивирусов (основанных на поиске известных программ), потому что их распространение лучше контролируется, и экземпляры программ попадают к специалистам антивирусной индустрии с бóльшей задержкой, нежели самопроизвольно распространяемые вредоносные программы. Однако эвристические (поиск алгоритмов) и проактивные (слежение) методы для них столь же эффективны.

# Вывод

Чтобы не попасться в руки злоумышленников, старайтесь избегать установки ненужных программ, перед установкой обязательно читать пользовательское соглашение, а так же, используйте антивирус, чтобы избежать случайного проникновения вируса в файлы ПК.

# Источники


- https://ru.wikipedia.org
- https://rucore.net/vse-o-stillerah-chto-eto-takoe-i-kak-im-polzovatsya/

# СПАСИБО ЗА ВНИМАНИЕ!