

Муниципальное общеобразовательное учреждение
ТСШ №1 с.Тюхтет Красноярский край

«Методы борьбы с компьютерными вирусами»

индивидуальный учебный проект

ВЫПОЛНИЛ:

ученик 11 класса

Козлов Кирилл Русланович

РУКОВОДИТЕЛЬ:

учитель

Анисимова Любовь Викторовна

Тюхтет, 2023

СОДЕРЖАНИЕ

Введение	3
1. Сущность компьютерного вируса / Классификация компьютерных вирусов	5-6
2. Терминология компьютерных вирусов / Классификация антивирусных программ	7-8
• Dr.Web	8
• Kaspersky	9
• Bitdefender	9-10
• Avast	10-11
• Norton	11
• Trend Micro	12
3. Признаки, по которым можно определить наличие вирусной программы в вашем ПК	13
4. Социальный опрос	14
5. Заключение	16
6. Источники информации	17

ВВЕДЕНИЕ

Актуальность темы:

По мере развития компьютерных систем и программного обеспечения возрастает объём и повышается риск заражения вирусами. Один из факторов, повысивший уязвимость данных - массовое производство мощных ЭВМ. Благодаря этой причине появились компьютерные вирусы. Более всего опасного в компьютерных вирусах заключается в том, что они могут искажать или уничтожать жизненно-важные информации, которые могут привести не только к временным или финансовым потерям, но и забрать с собой человеческие жизни.

Цель:

Выяснить, какими методами можно бороться с компьютерными вирусами.

Задачи:

Понять, что представляет собой компьютерный вирус. Его характер появления и распространения, знать способы борьбы с ними.

Гипотеза:

Благодаря существующим антивирусным программам, мы можем защитить информацию, хранящуюся на компьютере.

Методы исследования:

1. Поисковый
2. Опрос учащихся
3. Практический

Литературный обзор:

1. В наше время более 6.000 новых компьютерных вирусов создаётся и запускается каждый месяц.

2. Наиболее высокий риск подвергнуться атаке компьютерными вирусами — у США, за ними следует Россия.
3. Вы не заразите компьютер вирусом, лишь прочтя электронное письмо. Вредоносная программа активируется только при открытии ссылки или заражённого приложения к письму.
4. К 1990 году было известно порядка 50 компьютерных вирусов. В конце 1990-ых количество вирусов резко возросло до 48.000.

СУЩНОСТЬ КОМПЬЮТЕРНОГО ВИРУСА

Принято считать, что компьютерный вирус- программы или элементы программ, не санкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность самокопирования.

КЛАССИФИКАЦИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

- ***По среде обитания:***
 - Загрузочные
 - Файловые
 - Файлово-загрузочные
 - Сетевые
 - Системные

- ***По степени воздействия:***
 - Неопасные
 - Опасные
 - Очень опасные

- ***По способам заражения среды обитания:***
 - Резидентные
 - Нерезидентные

- ***По алгоритмической особенности построения:***
 - Репликаторы
 - Троянский конь
 - Логическая бомба
 - Мутанты
 - Невидимки
 - Макровирусы

ТЕРМИНОЛОГИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ

Червь (Worm) — это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети. Особенностью червей, отличающих их от других вирусов, является то, что они не несут в себе никакой вредоносной нагрузки, кроме саморазмножения, целью которого является замусоривание памяти, и как следствие, затормаживание работы операционной системы.

Троян или троянский конь (Trojans) - это программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируются программа, написанная только с одной целью — нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблагоприятных целях. (Считается самой опасной, т.к. в ней скрыты разные злоумышленные действия)

Зомби (Zombie) — это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное количество нежелательных сообщений электронной почты, а также распространяются вирусы и другие вредоносные программы.

Шпионская программа (Spyware) — это программный продукт, установленный или проникший на компьютер без согласия его владельца, с целью получения практически полного доступа к компьютеру, сбора и отслеживания личной или конфиденциальной информации. (В основном, эта программа проникает через сетевые черви, трояна или под видом рекламы)

Фишинг (Phishing) — это почтовая рассылка, имеющая своей целью получение конфиденциальной финансовой информации. Такое письмо, как правило, содержит ссылку на сайт, являющейся точной копией интернет-банка или другого финансового учреждения. Пользователь, обычно, не догадывается, что находится на фальшивом сайте и спокойно выдает злоумышленникам информацию о своих счетах, кредитных карточках, паролях и т. Д.

Фарминг – это вид мошенничества, при котором вредоносный код устанавливается на ПК или сервер жертвы. Этот код меняет информацию по IP-адресам, в результате чего обманутый пользователь перенаправляется на поддельные веб-сайты без их ведома и согласия. После того как пользователь переходит на поддельный сайт, ему предлагается ввести свою персональную информацию, которая затем будет использоваться против него.

КЛАССИФИКАЦИЯ АНТИВИРУСНЫХ ПРОГРАММ

1. Детекторы (сканеры)
2. Доктора (или фаги, дезинфекторы)
3. Ревизоры
4. Фильтры (сторожа, мониторы)
5. Иммунизаторы (вакцинаторы)

DR.WEB

Антивирус Dr.Web разработан российской компанией и входит в линейку лучших защитных утилит. Доктор Web быстро обнаруживает угрозу и в считанные секунды ее устраняет. Благодаря частым обновлениям, позволяет распознать даже самый новый вирус и современными методами шпионства. Однако, как и у любой программы, здесь также имеются свои минусы. Среди явных – это отсутствие функции очистки браузера и платное использование антивируса.

- **Плюсы:**

Мощная комплексная защита устройства от любого вида угроз;

Простой понятный интерфейс;

Широкая линейка продуктов – стационарный антивирус, портативная версия, для корпоративных целей, лечащая утилита, специальная программа для удаления и мобильная версия;

Минимальные системные требования и нагрузка на компьютер;

Вирусные базы регулярно обновляются и не требуют большого количества свободной памяти;

Возможность хранить важные файлы в собственном облачном хранилище от Dr.Web;

- **Минусы:**

Медленное копирование файлов

Кратковременная заморозка ОС

KASPERSKY

Все продукты «Лаборатории Касперского» для Windows отлично справляются с нейтрализацией вредоносного ПО и при этом не сильно влияют на производительность системы. А в программу начального уровня встроена даже защита от Ransomware. По этому показателю его превосходит только Bitdefender, бесплатная версия которого предлагает несколько больше возможностей. Разработана в России.

- **Плюсы:**

Прекрасная защита от вредоносного ПО

Менеджер паролей без ограничений

Новая встроенная защита от stalking

Низкое потребление ресурсов в фоновом режиме

- **Минусы:**

Ограничения VPN

В пакете начального уровня не так много функций

BITDEFENDER

Авторы большинства обзоров отмечают высокие показатели обнаружения вредоносных программ этого антивирусного ПО. Однако при

этом активное фоновое сканирование Bitdefender влияет на производительность системы. Поэтому на слабых ПК, находясь в интернете, не рекомендуется запускать какие-то другие приложения, кроме самых легких.

- **Плюсы:**

Надежная защита от вредоносного ПО

Расширенный пакет включает безлимитный VPN

Несколько дополнительных функций

Простой и удобный интерфейс

- **Минусы:**

Не поддерживает шифрования данных

Сильная фоновая загрузка системы

AVAST

Одно из самых известных бесплатных антивирусных приложений продолжает оставаться таковым, поддерживая и ряд платных функций, если пользователю нужно, например, поставить программу на несколько устройств или обеспечить дополнительную защиту.

- **Плюсы:**

Удобный интерфейс

Доступная цена

Минимальная нагрузка на систему при сканировании

- **Минусы:**

Интеллектуальное сканирование требует слишком большого внимания от пользователя из-за множества функций

Предлагает установить Google Chrome

NORTON

Любой продукт Norton обеспечивает отличную защиту от вредоносного ПО, а серьезная нагрузка на производительность системы с последними версиями стала намного меньше. В отличие от ряда других разработчиков антивирусного ПО, Norton не предлагает программ для безвозвратного уничтожения данных (шредеров), шифрования или конфиденциального веб-браузера ни в одном из своих пакетов.

- **Плюсы:**

Отличная защита от вредоносного ПО

Функция резервного копирования, облачное хранилище, менеджер паролей

Безлимитный VPN

Полноценная защита конфиденциальности

Минимальная потеря производительности при онлайн-сканировании

- **Минусы:**

Достаточно дорогое ПО

Нет уничтожителя и шифровальщика файлов

Значительные «тормоза» при полном сканировании, особенно на слабых системах

TREND MICRO

Trend Micro предлагает хорошую защиту, но его механизм обнаружения вредоносных программ плохо оптимизирован, поэтому создает большую нагрузку на систему во время сканирования. Кроме того, этот антивирус имеет значительное количество ложных срабатываний.

- **Плюсы:**

Хорошая защита от вредоносных программ

Безопасный браузер для покупок в интернете

Сканирование сайтов на угрозы личным данным

- **Минусы:**

Много ложных срабатываний на некоторых тестах

Сильный удар по производительности системы во время сканирования

Недостаточно дополнительных функций

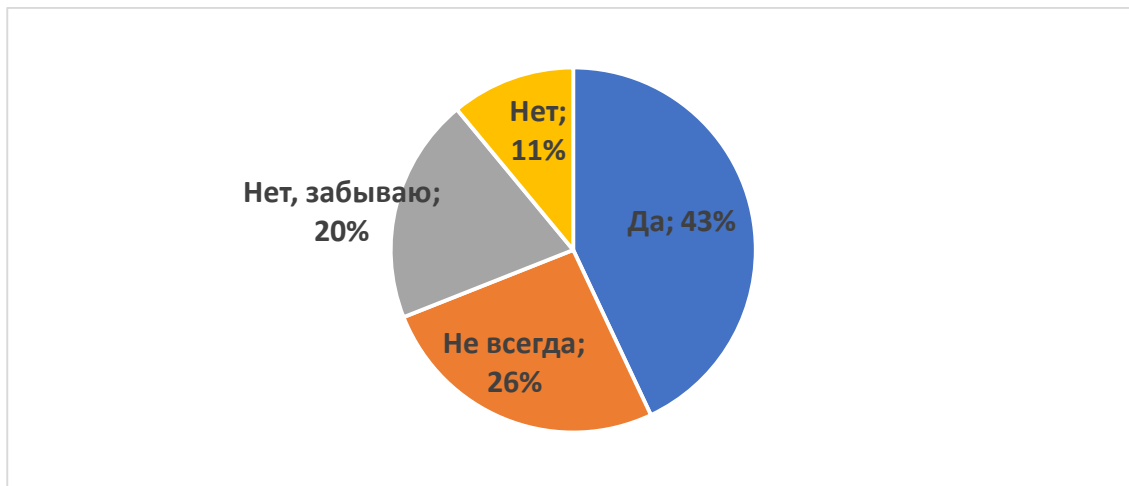
ПРИЗНАКИ, ПО КОТОРЫМ МОЖНО ОПРЕДЕЛИТЬ НАЛИЧИЕ ВИРУСНОЙ ПРОГРАММЫ В ВАШЕМ ПК

1. Медленная работа компьютера
2. Зависания и сбои в работе компьютера
3. Изменение размеров файлов
4. Уменьшение размера свободной оперативной памяти
5. Значительное увеличение количества файлов на диске
6. Исчезновение файлов и каталогов или искажение их содержимого
7. Изменение даты и времени модификации файлов

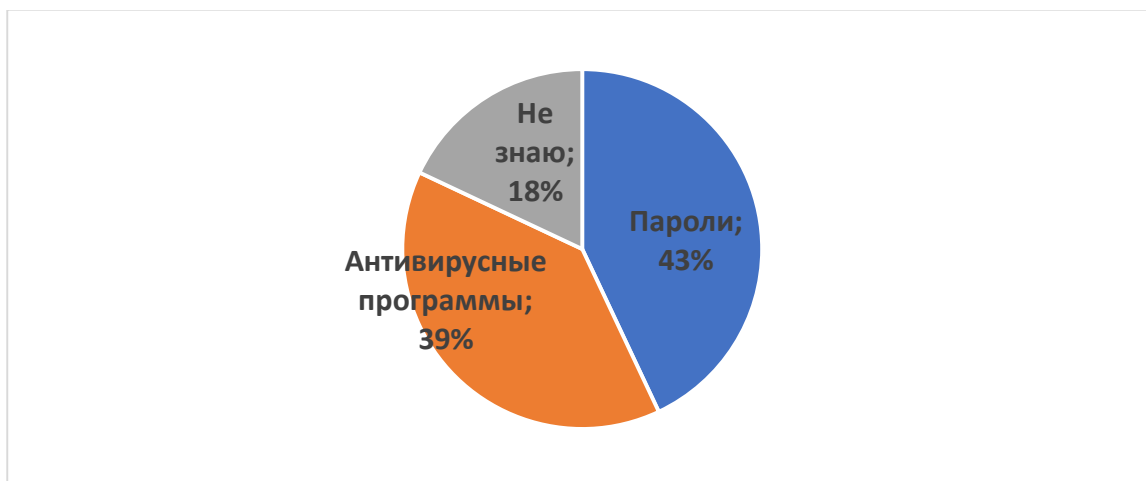
СОЦИАЛЬНЫЙ ОПРОС

В опросе приняли участие 241 житель с.Тюхтет.

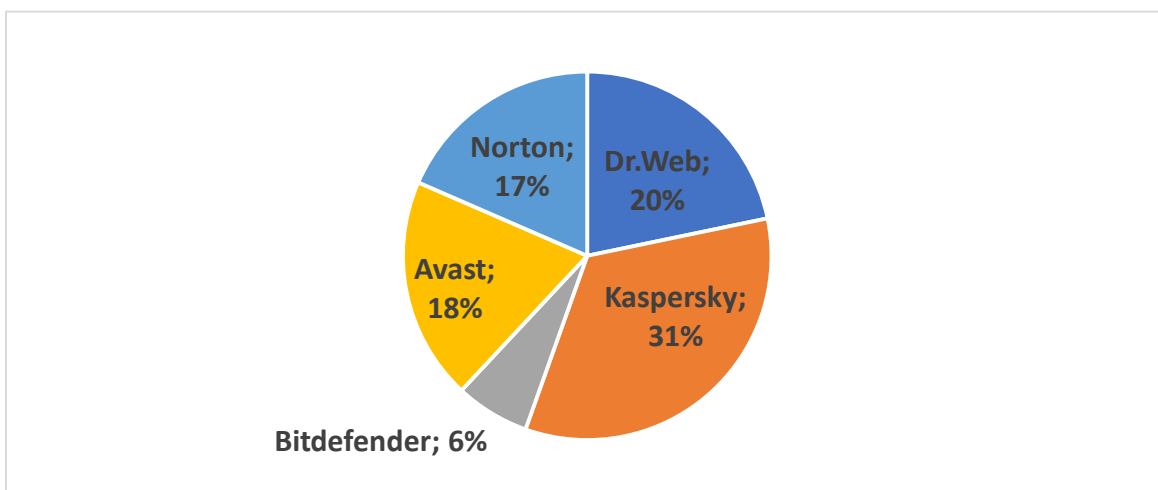
1. Выполняете ли Вы правила безопасной работы на компьютере?



2. Как Вы считаете, что является основной информационной безопасности



3. Какими антивирусными программами Вы пользуетесь



Вывод по опросу:

Исходя из результатов опроса можно сделать вывод

- Большинство опрошенных придерживаются безопасной работы за компьютером, многие считают, что пароли и антивирусные программы способны обезопасить их в информационной сфере.
- Большинство опрошенных людей предпочитают антивирусную программу - Kaspersky

ЗАКЛЮЧЕНИЕ

В наше время компьютерные вирусы живут по трем правилам: плодиться, прятаться и наносить вред. Практически все существующие антивирусные программы просты и удобны в пользовании, способны отлавливать почти все существующие сегодня группы вирусов. Большинство антивирусов способны не просто проверять по запросу пользователя диск на наличие вирусов, но и вести незаметную проверку всех запускаемых на компьютере файлов. Наконец, все современные антивирусы снабжены механизмом автоматического обновления антивирусных баз данных через Интернет.

Не исключено, что появятся и другие проблемы, которые принесут немало неприятностей пользователям и достаточное количество неурочной работы разработчикам антивирусных программ. Но все проблемы, когда-либо встававшие в истории развития вирусов, были довольно успешно решены. Скорее всего так же успешно будут решаться и будущие проблемы.

Вирусы успешно внедрились в повседневную компьютерную жизнь и покидать ее в обозримом будущем не собираются. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вирусов, способах заражения вирусами и защиты от них.

Источники информации

1. [Компьютерные вирусы \(reutov.ru\)](http://reutov.ru)
2. [Dr.Web \(официальный сайт\)](http://www.drweb.ru)
3. [Лаборатория Касперского \(официальный сайт\)](http://www.kaspersky.ru)
4. ВикибриФ [Bitdefender - Bitdefender](http://bitdefender.com)
5. [Avast](http://www.avast.com)
6. [Lumpics.ru](http://lumpics.ru). [Norton](http://norton.com)
7. [Trend Micro](http://trendmicro.com)
8. [Топ-25: Интересные факты про компьютерные вирусы, которые вам следует знать \(bugaga.ru\)](http://bugaga.ru)