Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/

Компьютерные вирусы и антивирусные программы

Юдинцева Наталия,
ученица 9А класса,
МАОУ СОШ № 54,
г. Новоуральск

Что такое компьютерный вирус?

- **Компьютерный вирус** — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.

Чем они опасны?

- Вирусы могут размножаться, и скрыто внедрять свои копии в файлы, загрузочные сектора дисков и документы. Активизация вируса может вызвать уничтожение программ и данных.. Первая эпидемия произошла в 1986г (вирус «Brain».) Всемирная эпидемия заражения почтовым вирусом началась 5 мая 2000 года, когда компьютеры по сети Интернет получили сообщения «Я тебя люблю» с вложенным файлом, который и содержал вирус.

Различные вирусы выполняют различные действия:

- Выводят на экран мешающие текстовые сообщения
- Создают звуковые эффекты
- Создают видео эффекты
- Замедляют работу ЭВМ, постепенно уменьшают объем свободной оперативной памяти;
- Увеличивают износ оборудования
- Вызывают отказ отдельных устройств, зависание или перезагрузку компьютера и крах работы всей ЭВМ;
- Уничтожают FAT, форматируют жесткий диск, стирают BIOS, уничтожают или изменяют данные, стирают антивирусные программы;

Разделение компьютерных вирусов по основным признакам:

- среда обитания
- особенности алгоритма
- способы заражения
- степень воздействия (безвредные, опасные, очень опасные)
- В зависимости от среды обитания основными типами компьютерных вирусов являются

Различные виды компьютерных вирусов:

- **Программные вирусы** – это вредоносный программный код, который внедрен внутрь исполняемых файлов (программ). Вирусный код может воспроизводить себя в теле других программ – этот процесс называется размножением.
- **Загрузочные вирусы** – поражают не программные файлы, а загрузочный сектор магнитных носителей (гибких и жестких дисков).
- **Макровирусы** – поражают документы, которые созданы в прикладных программах, имеющих средства для исполнения макрокоманд. К таким документам относятся документы текстового процессора WORD, табличного процессора Excel. Заражение происходит при открытии файла документа в окне программы, если в ней не отключена возможность исполнения макрокоманд.
- **Сетевые вирусы** пересылаются с компьютера на компьютер, используя для своего распространения компьютерные сети, электронную почту и другие каналы.

Как же защитить свой компьютер?

- Если компьютер необходимо срочно проверить на вирусы, лучше всего воспользоваться бесплатными утилитами Dr.Web CureIt! и Kaspersky Virus Removal Tool.
- Чтобы обеспечить постоянную защиту компьютера, установите антивирус с регулярным обновлением вирусных баз. Желательно настроить антивирус таким образом, чтобы он постоянно следил за поведением работающих на компьютере программ.
- Если у вас нет возможности установить платный антивирус, воспользуйтесь одной из бесплатных программ, перечисленных ниже. Большинство этих программ — пробные версии платных антивирусов, с урезанной функциональностью. Но даже такой антивирус сделает работу с интернетом безопаснее, чем его отсутствие.

Существуют бесплатные антивирусные программы:

- SUPERAntiSpyware
- Malwarebytes Anti-Malware
- AVG AntiVirus FREE
- AVZ
- Avast! Free Antivirus
- ClamWin
- Comodo Antivirus
- Microsoft Security Essentials
- NANO Антивирус
- Panda Cloud Antivirus
- Zillya! Антивирус
- 360 Total Security

Платные антивирусные программы:

- На российском рынке есть как платные, так и бесплатные антивирусы. Причем и тех, и других достаточно много, поэтому любой пользователь сможет подобрать себе антивирус по вкусу. Но когда есть широкий выбор, то бывает сложнее определиться, особенно человеку, не очень хорошо разбирающемуся в компьютерах, Интернет-технологиях и программном обеспечении.

8 способов избавиться от компьютерного вируса:

- Иногда бывает, что установленное у вас антивирусное ПО не может удалить какой-нибудь вирус или троянскую программу.
- 1. Попробуйте заменить антивирус
- 2. Используйте специальный сканер
- 3. Уничтожить вирус, зная его название
- 4. Проведите сканирование в безопасном режиме
- 5. Стоит переустановить систему
- 6. Запишите Live CD и запустите на вашем компьютере
- 7. Перенос жесткого диска на другой компьютер
- 8. Форматирование жесткого диска

Мобильные антивирусы

- В настоящее время с каждым днём увеличивается количество вредоносных приложений для операционной системы Android, направленных на хищения средств владельцев смартфонов, работающих на этой системе. В связи с этими тенденциями очень желательно использовать мобильные антивирусы для этой платформы, так как даже установка приложения из Google Play не гарантирует 100% антивирусную чистоту приложения.

Начнём с бесплатных вариантов:

- Trend Micro Dr. Safety для Android
- Антивирус Dr.Web Light для Android
- Kaspersky Internet Security для Android
- McAfee Mobile Security для Android.
- Bitdefender Antivirus Free для Android
- AVG AntiVirus FREE для Android.
- Avast Mobile Security для Android.
- Norton Mobile Security для Android.

Теперь переходим к платным версиям:

- ESET NOD32 Mobile Security для Android. Цена - 480 руб./год.
- Kaspersky Internet Security для Android. Цена - 300 руб./год.
- Dr.Web Security Space для Android. Цена от - 129 руб.
- Bitdefender Mobile Security для Android. Цена - 9.95 USD.

Как выбрать антивирус?

- Есть несколько критериев, которые помогут вам выбрать антивирус:
- уровень защиты
- потребление ресурсов
- удобство в использовании
- цена

Что следует учитывать владельцам смартфона?

- Владельцам смартфона с установленным антивирусом необходимо понимать, что антивирус не является полной гарантией отсутствия вируса на устройстве, а только значительно снижает его появление и функционирование.
- Поэтому необходимо не устанавливать приложения из недоверенных источников и не устанавливать Root доступ для смартфонов.
- Так же необходимо при возможности обновлять версию операционной системы Android, так как вместе с обновлением устраняются найденные уязвимости операционной системы, которыми могут воспользоваться злоумышленники.

Рейтинг топ-5 лучших антивирусов для российских пользователей 2014

- 1. **BitDefender** заслуженно попал на 1-ое место рейтинга, поскольку этот антивирус является одним из лучших для Windows 7 и 8.

- 2. **Norton** получил 2-ое место в рейтинге лучших антивирусов, которыми пользуются в России.

- 3. **Kaspersky** занял только 3-е место, хотя это чрезвычайно популярный антивирус в России

- 4. **AVG** получил 4-ое место в рейтинге лучших антивирусов для РФ.

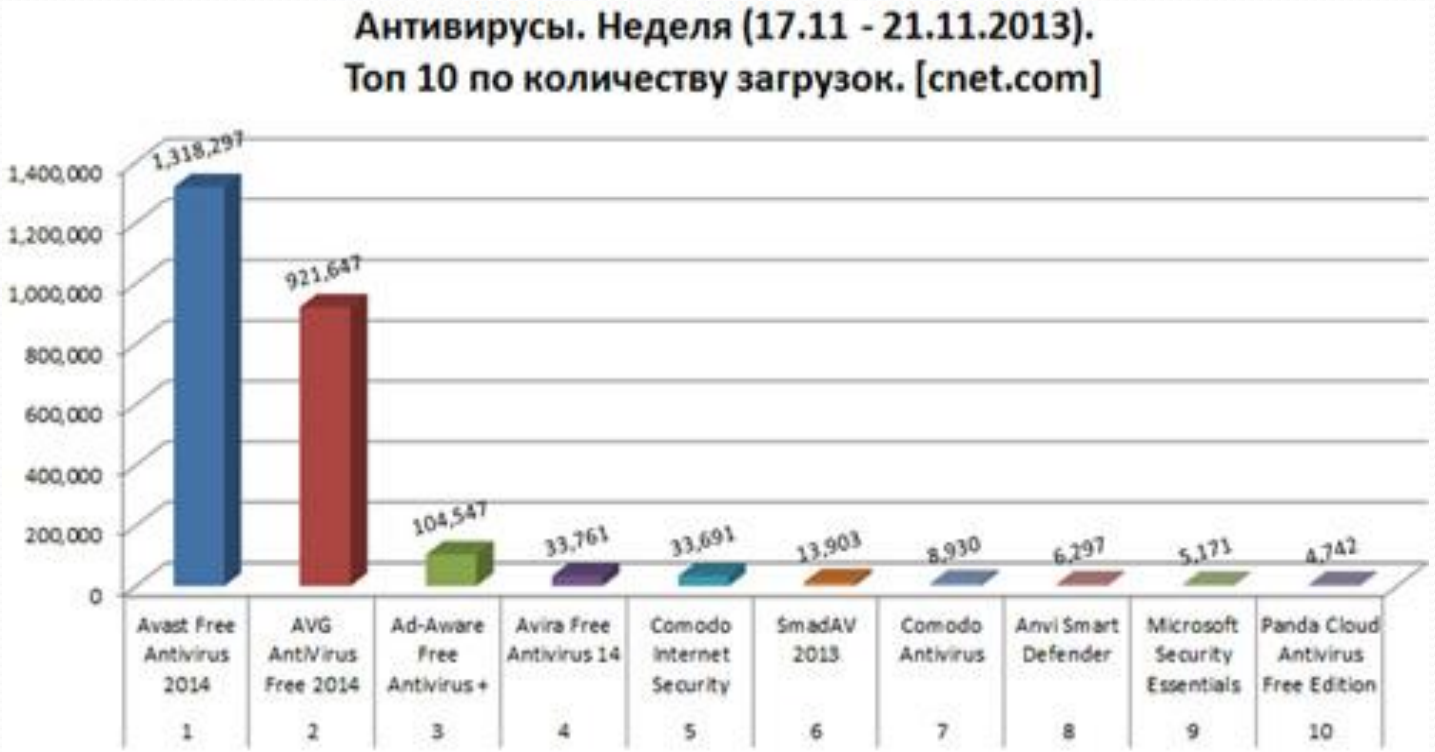
- 5. **Avast** закрывает пятерку лидеров рейтинга.

Немного статистики:

- Какие антивирусы чаще всего скачивают в России, Топ-10 антивирусов

Немного статистики:

- Какие антивирусы чаще всего скачивают в Европе, Топ-10 антивирусов



Рейтинг антивирусов,

август 2013 г.

№	Издатель: Антивирус	ЗАЩИТА	ПРОИЗВОДИТЕЛЬНОСТЬ	УДОБСТВО	БЕСПЛАТНЫЙ?
1	F-Secure: Internet Security 2013	6	4.5	5.5	Нет
2	Comodo: Internet Security Premium 6.2	6	5	4	Да
3	BullGuard: Internet Security 13.0	6	3.5	5.5	Нет
4	G Data: InternetSecurity 2014	6	4.5	5.5	Нет
5	Bitdefender: Internet Security 2013 & 2014	6	5.5	6	Нет
6	Kaspersky: Internet Security 2013 & 2014	5.5	5.5	6	Нет
7	Symantec: Norton Internet Security 2013	5.5	6	5.5	Нет
8	Avast: Free AntiVirus 8.0	5.5	3	6	Да
9	Trend Micro: Titanium Maximum Security 2013 & 2014	5.5	5	4	Нет
10	MicroWorld: eScan Internet Security Suite 14.0	5.5	3.5	5.5	Нет
11	McAfee: Internet Security 2013	5	3	6	Нет
12	Qihoo: 360 Internet Security 4.2	5	4.5	6	Да
13	AVG: Internet Security 2013	5	4.5	5.5	Нет
14	ESET: Smart Security 6.0	5	2	6	Нет
15	Panda Security: Cloud Antivirus FREE 2.2	5	3.5	5.5	Да
16	AVG: Anti-Virus Free Edition 2013	4.5	4.5	5.5	Да
17	Norman: Security Suite Pro 10.0 & 10.1	3.5	2	4.5	Нет
18	ThreatTrack: VIPRE Internet Security 2013	3.5	3	5.5	Нет
19	Avira: Internet Security 2013	3.5	3.5	5	Нет, есть и Free
20	Tencent: PC Manager 7.4 & 8.1	3	5	6	Да
21	Webroot: SecureAnywhere Complete 8.0	2.5	6	4	Нет
22	Kingsoft: Antivirus 2013	2.5	2.5	6	Да
23	Check Point: ZoneAlarm Free Antivirus + Firewall 11.0	2	3	6	Да
24	K7 Computing: Total Security 13.1	2	3.5	5	Нет
25	AhnLab: V3 Internet Security 8.0	1.5	3.5	5	Да
26	Microsoft: Security Essentials 4.2 & 4.3	0.5	5	6	Да

Что надо знать о современных компьютерных угрозах?

- Современные вирусы не так страшны, как их предшественники. Улучшенные механизмы защиты операционных систем часто не позволяют им творить тот же беспредел, что и раньше (например, форматирование винчестера). Вирусы и атаки мошенников теперь в основном направлены на получение финансовой выгоды или управление компьютером пользователя, но не на уничтожение данных. При этом для выполнения перечисленных задач не всегда даже требуется вирус, нередко достаточно правильно составленного письма или SMS, чтобы его получатель сам отправил сведения о кредитной карте или другую конфиденциальную информацию злоумышленникам. В базе сигнатур большинства антивирусов содержится несколько миллионов записей о различных вирусах, однако серьезную угрозу составляют не более 10 разных видов атак.

Способы проникновения на компьютер

- Сначала остановимся на самом механизме проведения атаки. Если речь идет о фишинге или социальной инженерии, то сообщения обычно приходят по чату в социальных сетях, электронной почте или на форумах. В ряде случаев злоумышленники могут размещать их со ссылкой на свой ресурс прямо в комментариях чужих сайтов. Если модераторы вовремя не успели их удалить, то некоторые пользователи перейдут по ссылке и попадутся на удочку мошенников.
  Когда хакеры пытаются установить вирус на чей-то компьютер, то в большинстве случаев им нужно, чтобы пользователь лично запустил программу. Чтобы убедить владельца ПК сделать это, вирус, как правило, выдают за какое-то полезное ПО. Например, критическое обновление для Windows, антивирус, кодек, необходимый для просмотра видео на сайте, и т. д. Вирусы также распространяются в крэках и генераторах ключей, но опасность этих файлов несколько преувеличена.

Зачем злоумышленникам информация о пользователях и доступ к их компьютеру

- Главных целей всего две. Достигаются они разными способами, но мошенников интересует либо получение денег от (суммы могут варьироваться в широких пределах), либо использование компьютера или аккаунтов его владельца для рассылки спама. Контроль над чужим ПК позволяет создавать ботнет-сети, в состав которых иногда входят сотни тысяч компьютеров. Такие виртуальные армии формируются для рассылки спама или DDOS-атак на сайты. Пользователи зачастую даже не подозревают о том, что их ПК управляет кто-то другой

Блокировка компьютера

- Весьма распространенной и в то же время довольно неприятной является атака, при которой злоумышленники блокируют компьютер, требуя отправить SMS для получения кода разблокировки. Причем владельцу ПК не всегда сообщают, сколько денег будет снято со счета. Как удалось выяснить, по крайней мере в ряде случаев речь идет о ~30$.
Попадают такие вирусы чаще всего на ПК неопытных пользователей, которые устанавливают на него программы (например, видеокодеки), предлагаемые при посещении сайтов мошенников.

Берегите свой компьютер!