КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

Презентация подготовлена для конкурса "Интернешка" http://interneshka.org/
Паньковой Анастасией Александровной
Ученици 10 «А» класса
МОБУ СОШ «№1»
Г. Арсеньев
2015г.



В наше время многие люди уже не представляют свою жизнь без компьютера. Пользователь современного персонального компьютера имеет свободный доступ ко всем ресурсам машины.

Сегодня массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации.

Что бы обезопасить и продлить жизнь своему компьютеру, нужно изначально позаботиться о его защите т.е подобрать хорошую и надежную антивирусную программу.

НО!!! для того что бы ее выбрать для начала необходимо узнать что же такое компьютерные вирусы, понять их сущность, узнать виды и направленность.

Итак, что такое компьютерный вирус и какова его цель?

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.

Как правило, целью вируса является нарушение работы программно-аппаратных комплексов:

- удаление файлов,
- приведение в негодность структур размещения данных,
- блокирование работы пользователей
- приведение в негодность аппаратных комплексов компьютера
- и т. п..

Даже если автор вируса не запрограммировал вредоносных эффектов, вирус может приводить к сбоям компьютера из-за ошибок, неучтённых тонкостей взаимодействия с операционной системой и другими программами.
Кроме того, вирусы, как правило, занимают место на накопителях информации и потребляют некоторые другие ресурсы системы.

Классификация

Ныне существует немало разновидностей вирусов, различающихся по основному способу распространения и функциональности.

Если изначально вирусы распространялись на дискетах и других носителях, то сейчас доминируют вирусы, распространяющиеся через Интернет. Растёт и функциональность вирусов, которую они перенимают от других видов программ.

Вирусы принято распределять:

- **по поражаемым операционным системам и платформам**
  - DOS
  - Unix
  - Microsoft Windows
  - Linux
- **По поражаемым объектам**
  - Файловые вирусы
  - Загрузочные вирусы
  - Сценарные вирусы
  - макровирусы
  - Вирусы, поражающие исходный код
- **по технологиям, используемым вирусом**
  - полиморфные
  - вирусы
  - стелс-вирусы
  - руткиты
- **по языку, на котором написан вирус**
  - ассемблер
  - Высокоуровневый язык программир.
  - Сценарный язык
  - И др.
- **По доп. Вредонос. Функцион.**
  - бэкдоры
  - кейлоггеры
  - Шпионы
  - ботнеты
  - И др.

По масштабу вредных воздействий компьютерные вирусы делятся на:

* ***Безвредные*** – не влияют на работу ПК, лишь уменьшают объем свободной памяти на диске, в результате своего размножения
* ***Неопасные*** – влияние, которых ограничивается уменьшением памяти на диске, графическими, звуковыми и другими внешними эффектами;
* ***Опасные*** – приводят к сбоям и зависаниям при работе на ПК;
* ***Очень опасные*** – приводят к потери программ и данных (изменение, удаление), форматированию винчестера и тд.

Механизм, каналы и отличительные особенности!

Вирусы распространяются, копируя свое тело и обеспечивая его последующее исполнение: внедряя себя в исполняемый код других программ, заменяя собой другие программы, прописываясь в автозапуск и другое. Вирусом или его носителем могут быть не только программы, содержащие машинный код, но и любая информация, содержащая автоматически исполняемые команды — например, пакетные файлы и документы Microsoft Word и Excel, содержащие макросы. Кроме того, для проникновения на компьютер вирус может использовать уязвимости в популярном программном обеспечении (например, Adobe Flash, Internet Explorer, Outlook), для чего распространители внедряют его в обычные данные (картинки, тексты и т. д.) вместе с эксплоитом, использующим уязвимость.

Каналы

- Дискеты.
- Флеш-накопители (флешки).
- Электронная почта.
- Системы обмена мгновенными сообщениями.
- Веб-страницы.

Интернет и локальные сети (черви*).

Отличительными особенностями компьютерных вирусов являются:

- маленький объем;
- самостоятельный запуск;
- многократное копирование кода;
- создание помех для корректной работы компьютера

***Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя.**

Антивирусные программы

Антивирусная программа (антивирус) — специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления заражённых (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

Для обнаружения, удаления и защиты от компьютерных вирусов разработано несколько видов специальных антивирусных программ:

— программы-детекторы;
— программы-доктора, или фаги;
— программы-ревизоры;
— программы-фильтры;
— программы-вакцины, или иммунизаторы.

Виды антивирусных программ

Программы-детекторы

Программы-доктора, или фаги, а также программы-вакцины

Программы-ревизоры

Программы-фильтры или

Вакцины или иммунизаторы

Базы антивирусов

Для использования антивирусов необходимы постоянные обновления так называемых баз антивирусов. Они представляют собой информацию о вирусах..

Поскольку вирусы пишут часто, то необходим постоянный монитори
активности вирусов в сети. Для этого существуют специальные сет
которые собирают соответствующую информацию. После сбора эт
информации производится анализ вредоносности вируса,
анализируется его код, поведение, и после этого устанавливаются
способы борьбы с ним.

Чаще всего вирусы запускаются вместе с операционной системой. В таком случае можно просто удалить строки запуска вируса из реестра, и на этом в простом случае процесс может закончиться.

Более сложные вирусы используют возможность заражения файлов. Например, известны случаи, как некие даже антивирусные программы, будучи зараженными, сами становились причиной заражения других чистых программ и файлов.

Таким образом, вирусы усложнились, как и усложнились способы борьбы с ними. Обычно такие вирусы пишут в языках программирования более высокого уровня, поэтому их легче остановить.

Но по-прежнему существует угроза от вирусов, написанных на низкоуровневых машинных кодах наподобие ассемблера. Сложные вирусы заражают операционную систему, после чего она становится уязвимой и нерабочей.

Рейтинг протестированных антивирусных программ

Agnitum

Продукт	Тест	Награда
Outpost Security Suite Pro 7.5.3	Лечение активного заражения	Тест провален
Outpost Security Suite Pro 7.5.1	Быстродействие (постоянная защита)	Серебро
Outpost Security Suite Pro 7.5.1	Быстродействие (сканирование)	Бронза
Outpost Security Suite Pro 7.5.1	Быстродействие (влияние на работу с офисным ПО)	Тест провален
Outpost Security Suite Pro 7.1	Лечение активного заражения	Тест провален
Outpost Security Suite Pro 7.1	Быстродействие (постоянная защита)	Золото
Outpost Security Suite Pro 7.1	Быстродействие (сканирование)	Золото
Outpost Security Suite Pro 7.1	Быстродействие (влияние на работу с офисным ПО)	Золото
Outpost Security Suite Pro 2010	Самозащита x64	Золото
Outpost Security Suite Pro 2010	Самозащита	Золото
Outpost Security Suite Pro 2009	Проактивная защита	Бронза
Outpost Antivirus Pro 2009	Лечение активного заражения	Тест провален
Outpost Antivirus Pro 2009	Быстродействие (постоянная защита)	Серебро
Outpost Antivirus Pro 2009	Быстродействие (сканирование)	Золото
Outpost Antivirus Pro 2009	Быстродействие (влияние на работу с офисным ПО)	Бронза

Avast Software

Продукт	Тест	Награда
Avast! Internet Security 2015	Лечение активного заражения	Серебро
Avast! Internet Security 7.0	Лечение активного заражения	Тест провален
Avast! Internet Security 7.0	Тест эргономичности (удобства использования) персональных антивирусов	Золото
Avast Internet Security 6	Быстродействие (постоянная защита)	Золото
Avast Internet Security 6	Быстродействие (сканирование)	Серебро
Avast Internet Security 6	Быстродействие (влияние на работу с офисным ПО)	Серебро
Avast Internet Security 6.0	Лечение активного заражения	Бронза
Avast Internet Security 6.0	Быстродействие (постоянная защита)	Платина
Avast Internet Security 6.0	Быстродействие (сканирование)	Серебро
Avast Internet Security 6.0	Быстродействие (влияние на работу с офисным ПО)	Золото
Avast Internet Security 5.0	Самозащита x64	Золото
Avast Internet Security 5.0	Самозащита	Золото
Avast Internet Security 5.0	Проактивная защита	Серебро
Avast Professional Edition 4.8	Лечение активного заражения	Серебро
Avast Antivirus Professional 4.8	Быстродействие (постоянная защита)	Платина
Avast Antivirus Professional 4.8	Быстродействие (сканирование)	Серебро
Avast Antivirus Professional 4.8	Быстродействие (влияние на работу с офисным ПО)	Золото

AVG Technologies

Продукт	Тест	Награда
AVG Internet Security 2015	Лечение активного заражения	Тест провален
AVG Internet Security 2012	Лечение активного заражения	Тест провален
AVG Internet Security 2012	Быстродействие (постоянная защита)	Бронза
AVG Internet Security 2012	Быстродействие (сканирование)	Золото
AVG Internet Security 2012	Быстродействие (влияние на работу с офисным ПО)	Серебро
AVG Internet Security Business Edition 2012	Быстродействие (сканирование)	Тест провален
AVG Internet Security Business Edition 2012	Быстродействие (влияние на работу с офисным ПО)	Тест провален
AVG Internet Security 2011	Лечение активного заражения	Бронза
AVG Internet Security 2011	Быстродействие (постоянная защита)	Платина
AVG Internet Security 2011	Быстродействие (сканирование)	Бронза
AVG Internet Security 2011	Быстродействие (влияние на работу с офисным ПО)	Бронза
AVG Internet Security 2011	Самозащита x64	Серебро
AVG Internet Security 9.0	Самозащита	Бронза
AVG Internet Security 9.0	Проактивная защита	Серебро
AVG Anti-Virus & Anti-Spyware 8.5.0.40	Лечение активного заражения	Тест провален
AVG Internet Security 9.0	Быстродействие (постоянная защита)	Золото
AVG Internet Security 9.0	Быстродействие (сканирование)	Серебро
AVG Internet Security 9.0	Быстродействие (влияние на работу с офисным ПО)	Золото

Avira

Продукт	Тест	награда
Avira Internet Security 14	Лечение активного заражения	Тест провален
Avira Internet Security 2012	Лечение активного заражения	Тест провален
Avira Premium SecuritySuite 2012	Быстродействие (постоянная защита)	Серебро
Avira Premium SecuritySuite 2012	Быстродействие (сканирование)	Серебро
Avira Premium SecuritySuite 2012	Быстродействие (влияние на работу с офисным ПО)	Бронза
Avira Premium Security Suite 10.0	Лечение активного заражения	Тест провален
Avira Premium Security Suite 10.0	Быстродействие (постоянная защита)	Платина
Avira Premium Security Suite 10.0	Быстродействие (сканирование)	Платина
Avira Premium Security Suite 10.0	Быстродействие (влияние на работу с офисным ПО)	Серебро
Avira Premium Security Suite 10.0	Самозащита x64	Серебро
Avira Premium Security Suite 10.0	Самозащита	Золото
Avira AntiVir Premium Security Suite 9.0	Проактивная защита	Тест провален
Avira AntiVir PE Premium 9.0	Лечение активного заражения	Тест провален
Avira Premium Security Suite 9.0	Быстродействие (постоянная защита)	Золото
Avira Premium Security Suite 9.0	Быстродействие (сканирование)	Платина
Avira Premium Security Suite 9.0	Быстродействие (влияние на работу с офисным ПО)	Золото

BitDefender

Продукт	Тест	Награда
BitDefender Internet Security 18	Лечение активного заражения	Серебро
BitDefender Internet Security 2013	Лечение активного заражения	Серебро
BitDefender Internet Security 2012	Быстродействие (постоянная защита)	Серебро
BitDefender Internet Security 2012	Быстродействие (сканирование)	Золото
BitDefender Internet Security 2012	Быстродействие (влияние на работу с офисным ПО)	Серебро
BitDefender Internet Security 2011	Лечение активного заражения	Тест провален
BitDefender Internet Security 2011	Быстродействие (постоянная защита)	Золото
BitDefender Internet Security 2011	Быстродействие (сканирование)	Золото
BitDefender Internet Security 2011	Быстродействие (влияние на работу с офисным ПО)	Серебро
BitDefender Internet Security 2011	Самозащита x64	Золото
BitDefender Internet Security 2011	Самозащита	Золото
BitDefender Internet Security 2010	Проактивная защита	Серебро
BitDefender Antivirus 2010	Лечение активного заражения	Тест провален
BitDefender Antivirus 2010	Быстродействие (постоянная защита)	Золото
BitDefender Antivirus 2010	Быстродействие (сканирование)	Золото
BitDefender Antivirus 2010	Быстродействие (влияние на работу с офисным ПО)	Золото

Comodo

Продукт	Тест	Награда
Comodo Internet Security 5.10	Лечение активного заражения	Тест провален
Comodo Internet Security 2012	Быстродействие (постоянная защита)	Бронза
Comodo Internet Security 2012	Быстродействие (сканирование)	Серебро
Comodo Internet Security 2012	Быстродействие (влияние на работу с офисным ПО)	Бронза
Comodo Internet Security 5.3	Лечение активного заражения	Тест провален
Comodo Internet Security 5.3	Быстродействие (постоянная защита)	Серебро
Comodo Internet Security 5.3	Быстродействие (сканирование)	Тест провален
Comodo Internet Security 5.3	Быстродействие (влияние на работу с офисным ПО)	Золото
Comodo Internet Security 5.0	Самозащита x64	Золото
Comodo Internet Security 4.1	Самозащита	Золото
Comodo Internet Security 4.0	Проактивная защита	Бронза
Comodo Antivirus 3.13	Лечение активного заражения	Тест провален

Доктор Веб

Продукт	Тест	Награда
Dr.Web Security Space Pro 10	Лечение активного заражения	Серебро
Dr.Web Security Space Pro 7	Лечение активного заражения	Золото
Dr.Web Security Space 7	Тест эргономичности (удобства использования) персональных антивирусов	Серебро
Dr.Web Security Space 7	Быстродействие (постоянная защита)	Платина
Dr.Web Security Space 7	Быстродействие (сканирование)	Тест провален
Dr.Web Security Space 7	Быстродействие (влияние на работу с офисным ПО)	Тест провален
Dr.Web Enterprise Suite 6.0	Быстродействие (сканирование)	Золото
Dr.Web Enterprise Suite 6.0	Быстродействие (влияние на работу с офисным ПО)	Тест провален
Dr.Web Security Space 6.0	Лечение активного заражения	Золото
Dr.Web Security Space 6.0	Быстродействие (постоянная защита)	Платина
Dr.Web Security Space 6.0	Быстродействие (сканирование)	Нет награды
Dr.Web Security Space 6.0	Быстродействие (влияние на работу с офисным ПО)	Бронза
Dr.Web Security Space 6.0	Самозащита x64	Золото
Dr.Web Security Space 6.0	Самозащита	Платина
Dr.Web Security Space 6.0	Проактивная защита	Бронза
Dr.Web Anti-Virus 5.0	Лечение активного заражения	Золото
Dr.Web 5.0	Быстродействие (постоянная защита)	Нет награды
Dr.Web 5.0	Быстродействие (сканирование)	Нет награды
Dr.Web 5.0	Быстродействие (влияние на работу с офисным ПО)	Серебро

Emsisoft

Продукт	Тест	Награда
Emsisoft Internet Security 9	Лечение активного заражения	Тест провален
Emsisoft Anti-Malware 5.1	Лечение активного заражения	Тест провален
Emsisoft Anti-Malware 5.1	Быстродействие (постоянная защита)	Золото
Emsisoft Anti-Malware 5.1	Быстродействие (сканирование)	Бронза
Emsisoft Anti-Malware 5.1	Быстродействие (влияние на работу с офисным ПО)	Без награды
Emsisoft Anti-Malware 5.0	Самозащита x64	Серебро

Eset

Продукт	Тест	Награда
Eset Smart Security 8.0	Лечение активного заражения	Тест провален
Eset Smart Security 5.2	Лечение активного заражения	Тест провален
Eset Smart Security 5.2	Тест эргономичности (удобства использования) персональных антивирусов	Золото
Eset Smart Security 5.0	Быстродействие (постоянная защита)	Бронза
Eset Smart Security 5.0	Быстродействие (сканирование)	Бронза
Eset Smart Security 5.0	Быстродействие (влияние на работу с офисным ПО)	Золото
ESET Smart Security 4.2 Business Edition	Быстродействие (сканирование)	Бронза
ESET Smart Security 4.2 Business Edition	Быстродействие (влияние на работу с офисным ПО)	Платина
Eset Smart Security 4.2	Лечение активного заражения	Тест провален
Eset Smart Security 4.2	Быстродействие (постоянная защита)	Платина
Eset Smart Security 4.2	Быстродействие (сканирование)	Серебро
Eset Smart Security 4.2	Быстродействие (влияние на работу с офисным ПО)	Золото
Eset Smart Security 4.2	Самозащита x64	Бронза
Eset Smart Security 4.2	Самозащита	Серебро
Eset Smart Security 4.0	Проактивная защита	Бронза
Eset Nod32 Antivirus 4.0	Лечение активного заражения	Тест провален
Eset Nod32 Antivirus 4.0	Быстродействие (постоянная защита)	Бронза
Eset Nod32 Antivirus 4.0	Быстродействие (сканирование)	Бронза
Eset Nod32 Antivirus 4.0	Быстродействие (влияние на работу с офисным ПО)	Золото

F-Secure

Продукт	Тест	Награда
F-Secure Internet Security 2012	Лечение активного заражения	Тест провален
F-Secure Internet Security 2012	Быстродействие (постоянная защита)	Бронза
F-Secure Internet Security 2012	Быстродействие (сканирование)	Золото
F-Secure Internet Security 2012	Быстродействие (влияние на работу с офисным ПО)	Бронза
F-Secure Internet Security 2011	Лечение активного заражения	Бронза
F-Secure Internet Security 2011	Быстродействие (постоянная защита)	Золото
F-Secure Internet Security 2011	Быстродействие (сканирование)	Золото
F-Secure Internet Security 2011	Быстродействие (влияние на работу с офисным ПО)	Без награды
F-Secure Internet Security 2011	Самозащита x64	Серебро
F-Secure Internet Security 2010	Самозащита	Бронза
F-Secure Internet Security 2010	Проактивная защита	Тест провален
F-Secure Anti-Virus 2010	Лечение активного заражения	Бронза
F-Secure Internet Security 2010	Быстродействие (постоянная защита)	Серебро
F-Secure Internet Security 2010	Быстродействие (сканирование)	Золото
F-Secure Internet Security 2010	Быстродействие (влияние на работу с офисным ПО)	Без награды

Лаборатория Касперского

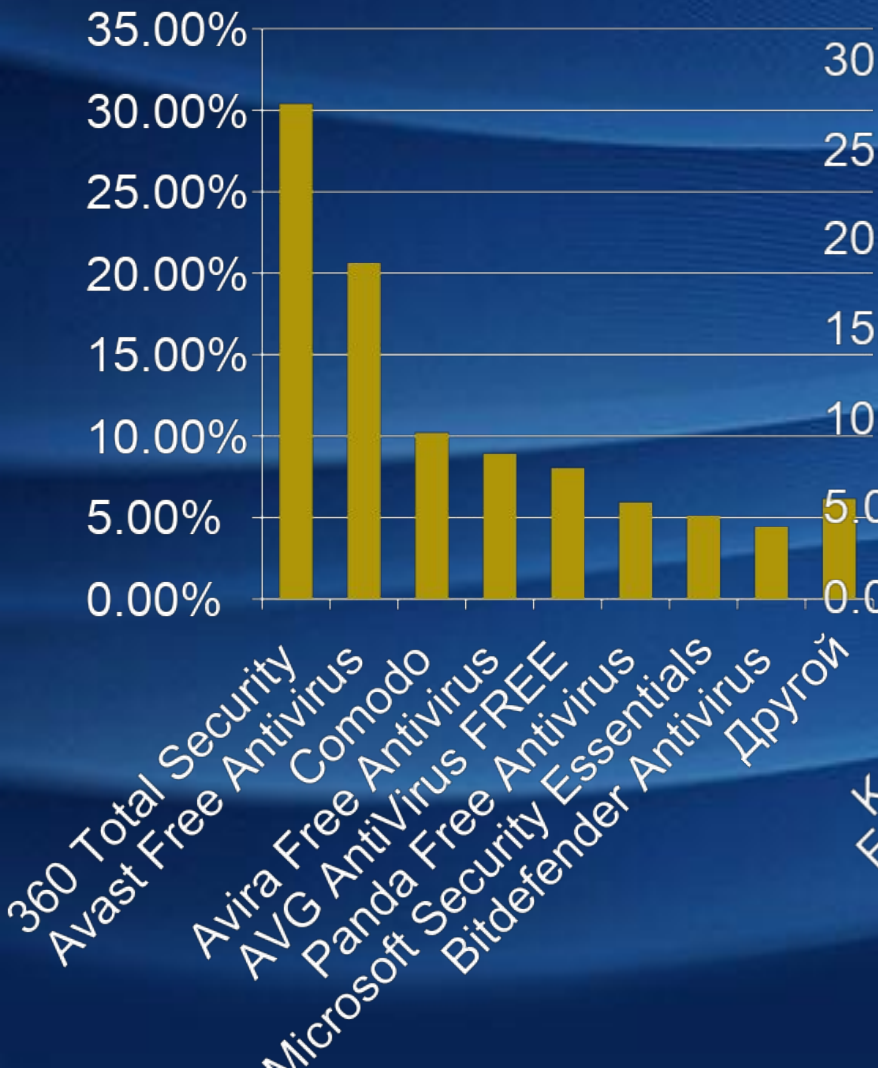
Продукт	Тест	Награда
Kaspersky Internet Security 15	Лечение активного заражения	Платина
Kaspersky Internet Security 2012	Лечение активного заражения	Платина
Kaspersky Internet Security 2012	Тест эргономичности (удобства использования) персональных антивирусов	Золото
Kaspersky Internet Security 2012	Быстродействие (постоянная защита)	Золото
Kaspersky Internet Security 2012	Быстродействие (сканирование)	Золото
Kaspersky Internet Security 2012	Быстродействие (влияние на работу с офисным ПО)	Серебро
Kaspersky Endpoint Security 8.1	Быстродействие (сканирование)	Серебро
Kaspersky Endpoint Security 8.1	Быстродействие (влияние на работу с офисным ПО)	Тест провален
Kaspersky Internet Security 2011	Лечение активного заражения	Платина
Kaspersky Internet Security 2011	Быстродействие (постоянная защита)	Платина
Kaspersky Internet Security 2011	Быстродействие (сканирование)	Золото
Kaspersky Internet Security 2011	Быстродействие (влияние на работу с офисным ПО)	Серебро
Kaspersky Internet Security 2011	Самозащита x64	Платина
Kaspersky Internet Security 2011	Самозащита	Платина
Kaspersky Internet Security 2010	Проактивная защита	Серебро
Kaspersky Anti-Virus 2010	Лечение активного заражения	Золото
Kaspersky Anti-Virus 2010	Быстродействие (постоянная защита)	Золото
Kaspersky Anti-Virus 2010	Быстродействие (сканирование)	Золото
Kaspersky Anti-Virus 2010	Быстродействие (влияние на работу с офисным ПО)	Нет награды

Microsoft

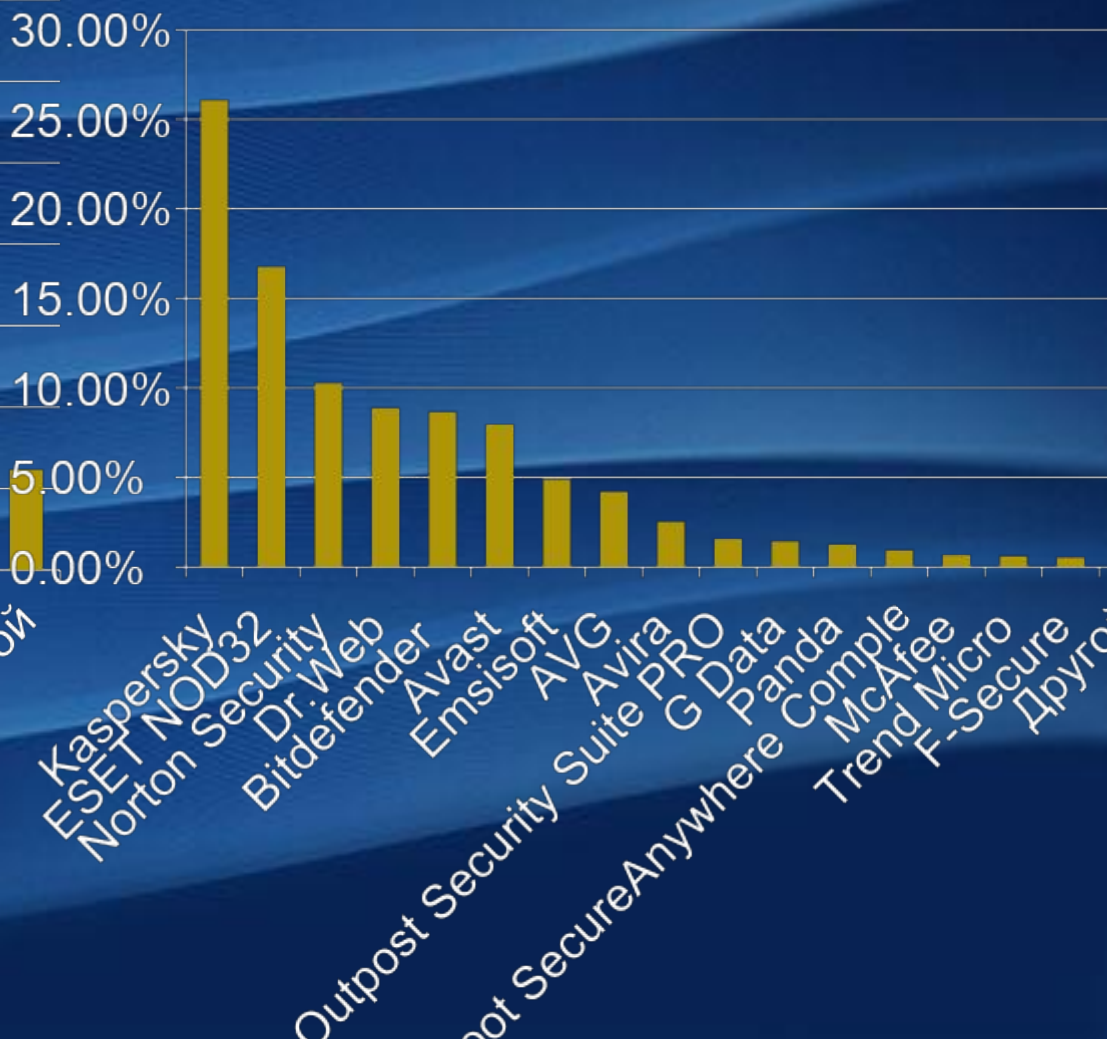
Продукт	Тест	Награда
Microsoft Security Essentials 4.6	Лечение активного заражения	Бронза
Microsoft Security Essentials 4.0	Лечение активного заражения	Бронза
Microsoft Security Essentials 2.1	Быстродействие (постоянная защита)	Тест провален
Microsoft Security Essentials 2.1	Быстродействие (сканирование)	Тест провален
Microsoft Security Essentials 2.1	Быстродействие (влияние на работу с офисным ПО)	Золото
Microsoft Security Essentials 2.0	Лечение активного заражения	Серебро
Microsoft Security Essentials 2.0	Быстродействие (постоянная защита)	Без награды
Microsoft Security Essentials 2.0	Быстродействие (сканирование)	Без награды
Microsoft Security Essentials 2.0	Быстродействие (влияние на работу с офисным ПО)	Золото
Microsoft Security Essentials 1.0	Самозащита x64	Тест провален
Microsoft Security Essentials 1.0	Самозащита	Тест провален
Microsoft Security Essentials 1.0	Проактивная защита	Серебро
Microsoft Security Essentials 1.0	Лечение активного заражения	Серебро
Microsoft Security Essentials 1.0	Быстродействие (постоянная защита)	Нет награды
Microsoft Security Essentials 1.0	Быстродействие (сканирование)	Нет награды
Microsoft Security Essentials 1.0	Быстродействие (влияние на работу с офисным ПО)	Золото

Лучший антивирус 2015 для Windows. Выбор пользователей

Лучший бесплатный антивирус 2015



Лучший комплексный антивирус 2015



Профилактика и лечение

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками.

Поэтому следует придерживаться некоторых мер предосторожности, в частности:

Не работать под привилегированными учётными записями без крайней необходимости (Учётная запись администратора в Windows);

Не запускать незнакомые программы из сомнительных источников;

Стараться блокировать возможность несанкционированного изменения системных файлов;

Отключать потенциально опасную функциональность системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.);

Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя;

Пользоваться только доверенными дистрибутивами*;

Постоянно делать резервные копии важных данных, желательно на носители, которые не стираются (например, BD-R) и иметь образ системы со всеми настройками для быстрого развёртывания;

Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.

Дистрибутив—это форма распространения программного обеспечения. Дистрибутив обычно содержит программы для начальной инициализации системы.

Источники

конец

- http://informatika.sch880.ru/p16aa1.html
- http://works.tarefer.ru/69/100023/index.html
- http://shkolo.ru/antivirusyi/
- https://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D0%B0%D1%8F_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B0
- https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D0%B9_%D0%B2%D0%B8%D1%80%D1%83%D1%81#.D0.9A.D0.BB.D0.B0.D1.81.D1.81.D0.B8.D1.84.D0.B8.D0.BA.D0.B0.D1.86.D0.B8.D1.8F
- http://www.anti-malware.ru/tests_history#agnitum
- https://www.anti-malware.ru/tests_history
- http://www.comss.ru/page.php?id=2426