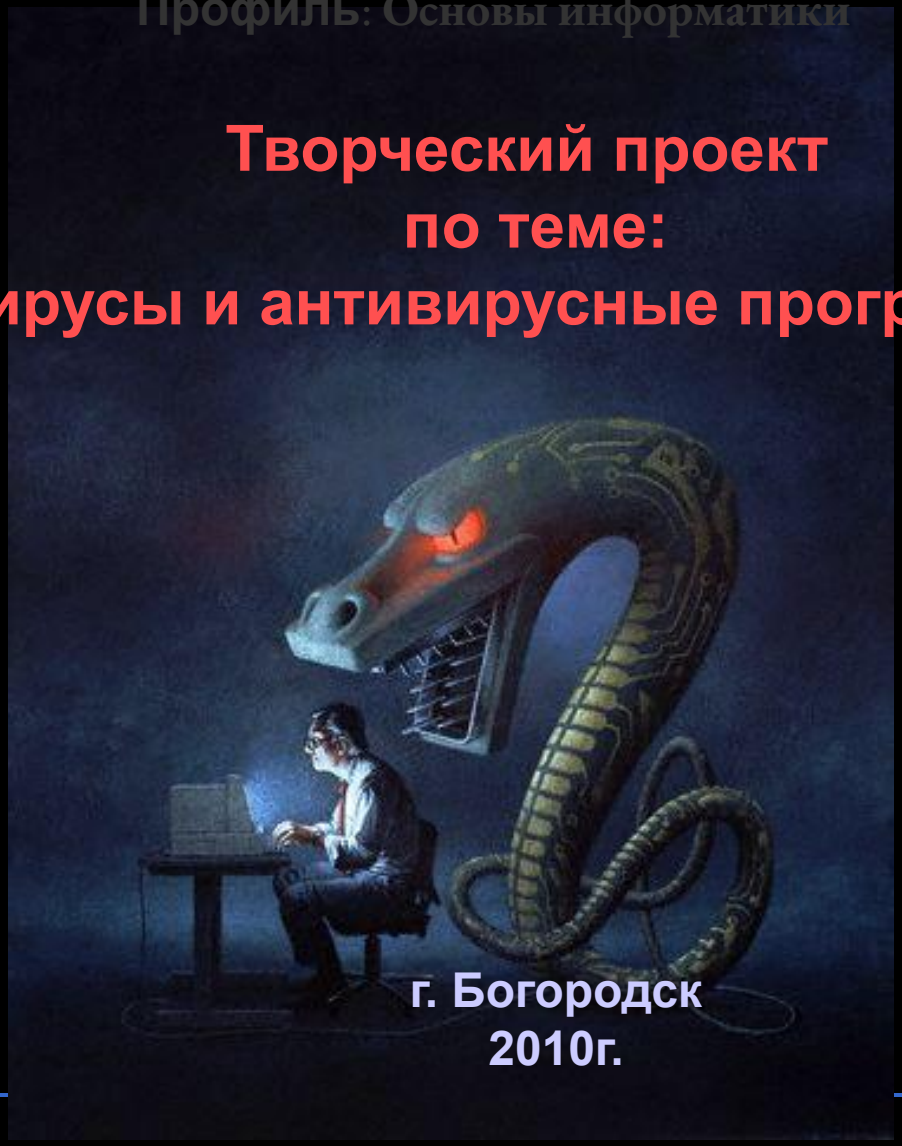
МОУ
Межшкольный учебный комбинат

Профиль: Основы информатики

Творческий проект по теме: «Вирусы и антивирусные программы".



Выполнила
учащаяся 10 кл. «а»
школы № 1
Шекурова Ксения

Проверила
Вострякова Е. А.

г. Богородск
2010г.

Содержание

Что такое вирусы?

Вирусы - программы или элементы программ, несанкционированно проникшие в компьютер с целью нанесения вреда, отличительной особенностью которых является способность самотиражирования. Наибольшая опасность таких вирусов заключается в том, что прежде чем нанести вред компьютеру и самообнаружиться, они копируются в другие программные файлы

Классификация вирусов

- *по среде обитания*
- *по способу заражения среды обитания*
- *по степени воздействия*
- *по свойствам алгоритма*

По среде обитания вирусы подразделяются на:

- ***Сетевые вирусы*** распространяются по различным компьютерным сетям.
- ***Файловые вирусы*** внедряются главным образом в исполняемые модули, т. е. В файлы, имеющие расширения COM и EXE.
- ***Загрузочные вирусы*** внедряются в загрузочный сектор диска (Boot-сектор) или в сектор, содержащий программу загрузки системного диска (Master Boot Re-cord).
- ***Файлово-загрузочные вирусы*** заражают как файлы, так и загрузочные сектора дисков.

По способу заражения среды обитания вирусы подразделяются на:

- *резидентные:*

  при заражении компьютера оставляет в оперативной памяти свою резидентную часть, которая потом перехватывает обращение операционной системы к объектам заражения (файлам, загрузочным секторам дисков и т. п.) и внедряется в них. Резидентные вирусы находятся в памяти и являются активными вплот до выключения или перезагрузки компьютера.

- *нерезидентные:*

  не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы подразделяются на:

- ***неопасные***, *не мешающие работе компьютера, но уменьшающие объем свободной оперативной памяти и памяти на дисках, действия таких вирусов проявляются в каких-либо графических или звуковых эффектах*

- ***опасные вирусы***, *которые могут привести к различным нарушениям в работе компьютера*

- ***очень опасные***, *воздействие которых может привести к потере программ, уничтожению данных, стиранию информации в системных областях диска.*

По особенностям алгоритма:

- **Простейшие вирусы - паразитические**, они изменяют содержимое файлов и секторов диска и могут быть достаточно легко обнаружены и уничтожены.
- **Вирусы-репликаторы**, называемые червями, которые распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии.
- **Вирусы-невидимки**, называемые **стелс-вирусами**, очень трудно обнаружить и обезвредить - они перехватывают обращения операционной системы к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска.
- **Вирусы-мутанты –** вирусы, содержащие алгоритмы шифровки-расшифровки, благодаря которым копии одного и того же вируса не имеют ни одной повторяющейся цепочки байтов, их наиболее трудно обнаружить.
- **Квазивирусные или «троянские» программы**, которые не способны к самораспространению, но очень опасны, так как, маскируясь под полезную программу, разрушают загрузочный сектор и файловую систему дисков.

Виды вирусов:

Троянский конь (Trojans)

Зомби (Zombie)

Червь (Worm)

Руткиты

Шпион (Spyware)

Фишинг (Phishing)

Фарминг

Троян или троянский конь (Trojans)

Троян или троянский конь (Trojans) - это программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируются программа, написанная с целью нанести ущерб целевому компьютеру путем выполнения несанкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

Зомби (Zombie)

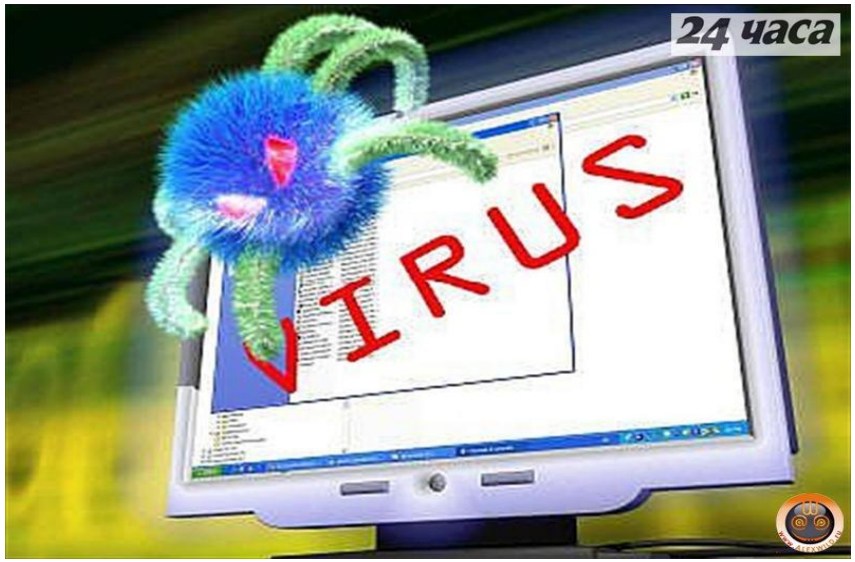
Зомби (Zombie) - это программа-вирус, которая после проникновения в компьютер, подключенный к сети Интернет управляется извне и используется злоумышленниками для организации атак на другие компьютеры. Зараженные таким образом компьютеры-зомби могут объединяться в сети, через которые рассылается огромное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

Червь (Worm)

Червь (Worm) - это программа, которая тиражируется на жестком диске, в памяти компьютера и распространяется по сети. Особенностью червей 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.

Руткиты

Руткиты – программы, установленные и работающие на компьютере без ведома пользователя и прячущие используемые злоумышленниками инструменты от антивирусного ПО. Они представляют значительный риск безопасности для домашних и корпоративных машин и сетей, так как их очень сложно обнаружить. Сами руткиты обычно устанавливаются с помощью вирусов или других вредоносных объектов, поэтому настоятельно рекомендуется постоянно обновлять антивирусную защиту и защиту от шпионов.



Шпионская программа (Spyware)

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. Эти программы, как правило, проникают на компьютер при помощи сетевых червей, троянских программ или под видом рекламы (adware).

Фишинг (Phishing)

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

Фарминг – замаскированная форма фишинга, заключающаяся в том, что при попытке зайти на официальный сайт интернет банка или коммерческой организации, пользователь автоматически перенаправляется на ложный сайт, который очень трудно отличить от официального сайта. Фарминг отличается от фишинга тем, что вместо электронной почты мошенники используют более изощренные методы направления пользователя на фальшивый сайт.

Виды Антивирусов

Антивирусы-
-фильтры

Антивирусы-
-детекторы

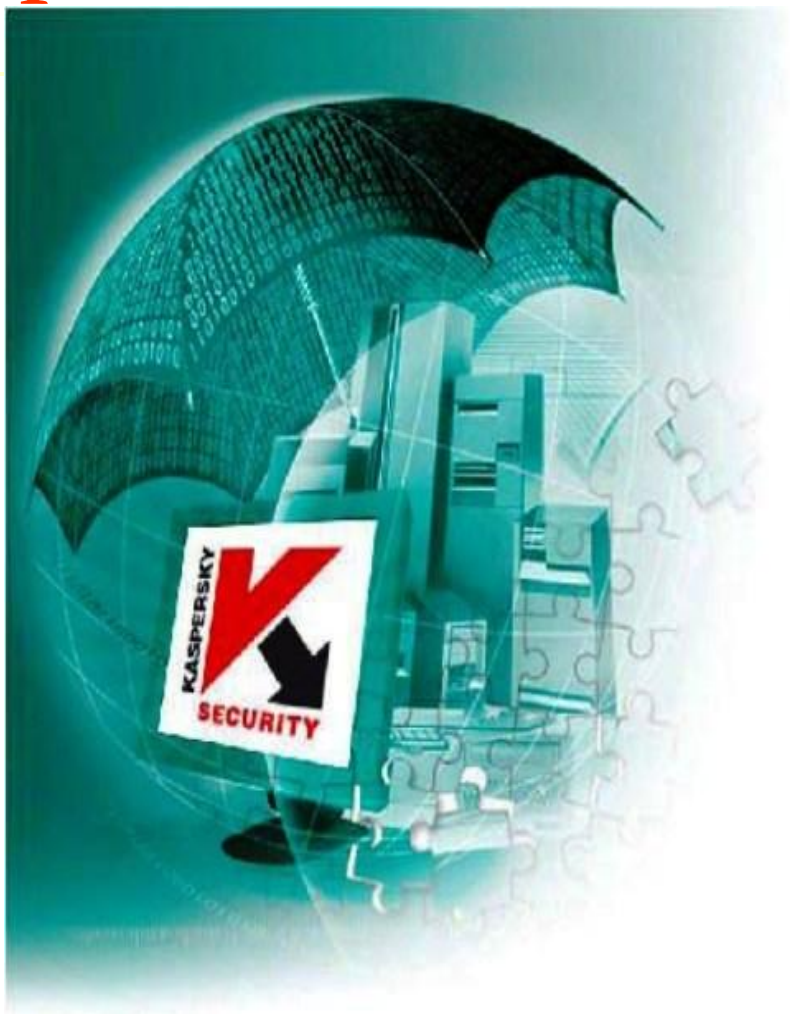
Антивирусы-
-вакцинаторы

Антивирусы-фильтры

Антивирусы-фильтры или сторожа **- п**рограммы, которые уведомляют пользователя обо всех действиях на его компьютере. Если вирус попытается проникнуть на ваш ПК или, наоборот, украсть пароль и отправить его злоумышленнику, сторож спросит: «Разрешить или запретить выполнение операции?». К сожалению, работа с данным типом защиты требует определённых навыков, ведь далеко не каждый знает, что обозначает тот или иной процесс.

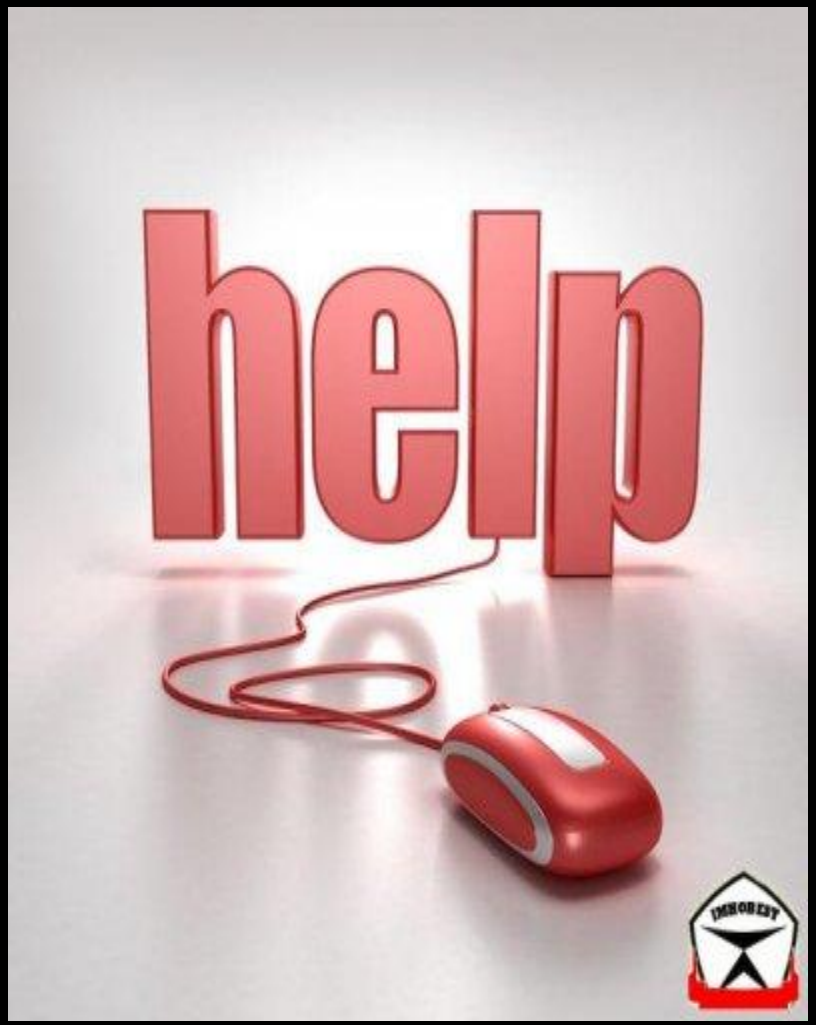
Антивирусы-детекторы

Антивирусы-детекторы нужно регулярно обновлять, ведь вредоносные программы быстро мутируют и размножаются. Какой антивирус-детектор лучше – не знает никто, хотя в интернете можно найти многочисленные тесты и сравнительные обзоры антивирусов. И дело не в стоимости, стране-производителе или размере баз для обновления. Главное почаще обновлять его и не забывать продлевать лицензию.



Антивирусы-вакцинаторы

Уже заражённые компьютеры сложно вылечить с помощью детектора или фильтра. В очень тяжёлых случаях на помощь приходят программы-вакцинаторы. Даже дорогой лицензионный антивирус не всегда может справиться с червём или троянской программой. К числу наиболее популярных вакцинаторов относятся Anti Trojan Elite, Trojan Remover или Dr.Web CureIt!. Последний, кстати, лечит практически любую инфицированную систему, но для регулярной защиты ПК его недостаточно.



Примеры антивирусных программ:

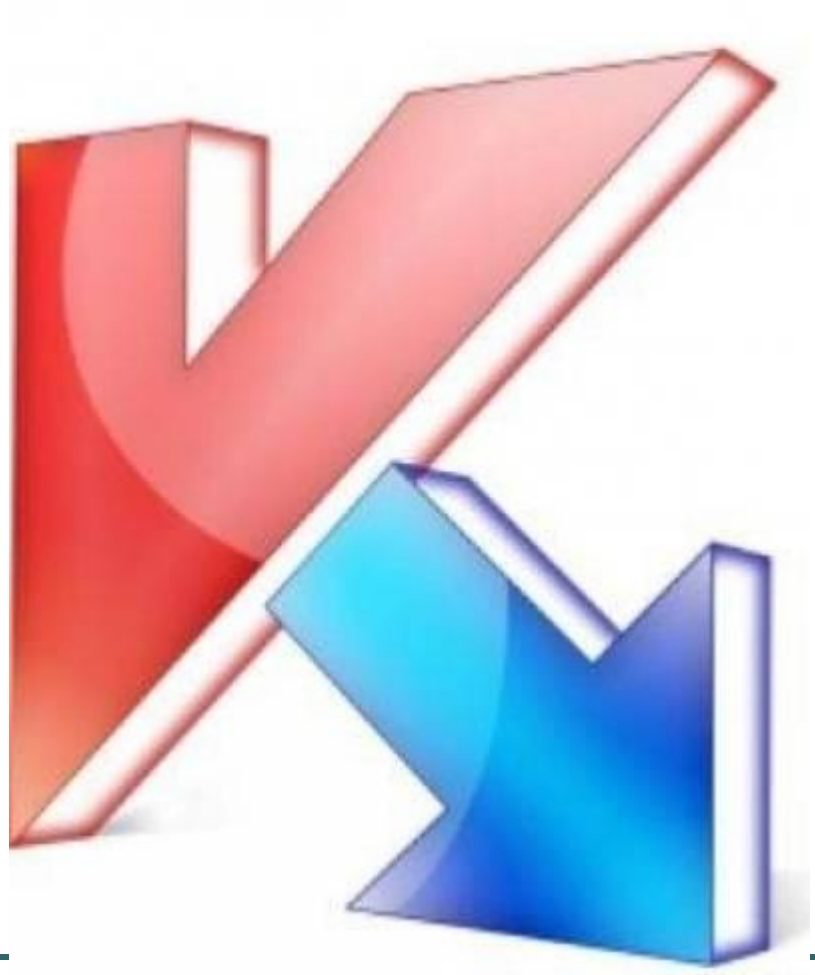
Антивирус Касперского

ESET NOD32

Dr. Web

Антивирус Касперского

Антивирус Касперского — антивирусное программное обеспечение, разрабатываемое Лабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS.

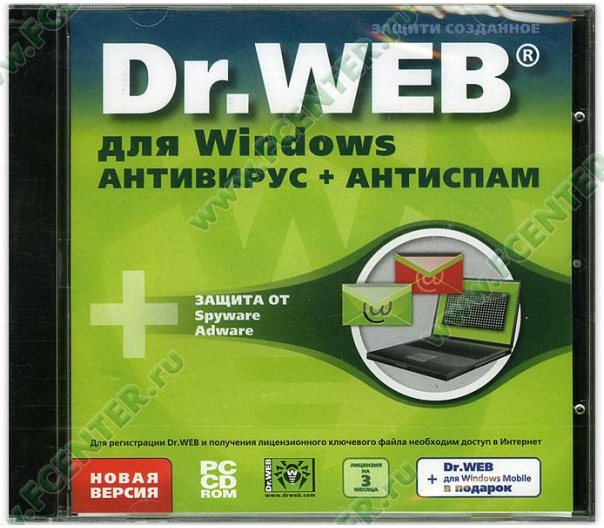


Антивирус NOD32

Проактивная защита и точное обнаружение угроз. Антивирус ESET NOD32 разработан на основе передовой технологии ThreatSense®. Ядро программы обеспечивает проактивное обнаружение всех типов угроз и лечение зараженных файлов (в том числе, в архивах) благодаря широкому применению интеллектуальных технологий, сочетанию эвристических методов и традиционного сигнатурного детектирования.

Dr.Web

Dr.Web — это семейство антивирусов, предназначенных для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама, скаминг-, фарминг-, фишинг-сообщений и технического спама.



THE END