РАЗНОВИДНОСТИ КОМПЬЮТЕРНЫХ ВИРУСОВ И МЕТОДЫ ЗАЩИТЫ ОТ НИХ. ОСНОВНЫЕ АНТИВИРУСНЫЕ ПРОГРАММЫ.

Подготовила:
учащаяся гр. П-7 I курса
Шарова Екатерина

СОДЕРЖАНИЕ

- Введение
- Компьютерные вирусы и их разновидности
- Методы защиты
- Основные антивирусные программы
- Использованная литература

Введение

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.

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.

Компьютерные вирусы и их разновидности

Компьютерным вирусом называется рукотворная программа, способная самостоятельно создавать свои копии и внедряться в другие программы, в системные области дисковой памяти компьютера, распространяться по каналам связи с целью прерывания и нарушения работы программ, порчи файлов, файловых систем и компонентов компьютера, нарушения нормальной работы пользователей.

Компьютерным вирусам, как и биологическим, характерны определенные стадии существования:

1. Латентная стадия, в которой вирусом никаких действий не предпринимается;
2. Инкубационная стадия, в которой основная задача вируса - создать как можно больше своих копий и внедрить их в среду обитания;
3. Активная стадия, в которой вирус, продолжая размножаться, проявляется и выполняет свои деструктивные действия.

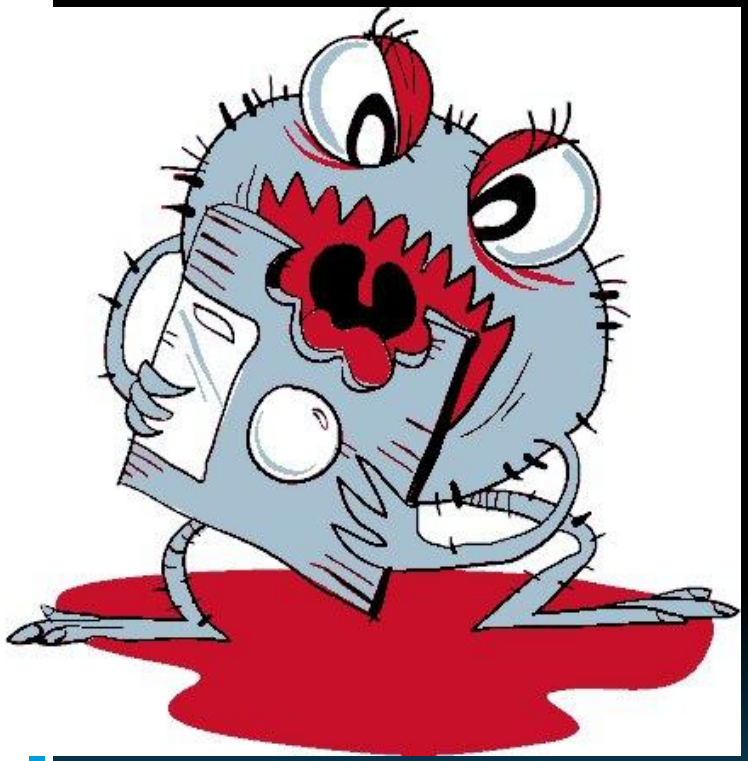
По среде обитания вирусы можно разделить на:

1.файловые;
2.загрузочные;
3.файлово-загрузочные;
4.сетевые;
5.документные.

Файловые вирусы

Файловые вирусы чаще всего внедряются в исполняемые файлы, имеющие расширения .exe и .com (самые распространенные вирусы), но могут внедряться и в файлы с компонентами операционных систем, драйверы внешних устройств, объектные файлы и библиотеки, в командные пакетные файлы, программные файлы на языках процедурного программирования.

Загрузочные вирусы



Загрузочные вирусы внедряются в загрузочный сектор дискеты (boot-sector) или в сектор, содержащий программу загрузки системного диска (master boot record). При загрузке DOS с зараженного диска такой вирус изменяет программу начальной загрузки либо модифицируют таблицу размещения файлов на диске, создавая трудности в работе компьютера или даже делая невозможным запуск операционной системы.

Файлово-загрузочные и сетевые вирусы

Файлово-загрузочные вирусы интегрируют возможности двух предыдущих групп и обладают наибольшей "эффективностью" заражения.

Сетевые вирусы используют для своего распространения команды и протоколы телекоммуникационных систем (электронной почты, компьютерных сетей).

Документные вирусы

Документные вирусы (их часто называют макровирусами) заражают и искажают текстовые файлы (.doc) и файлы электронных таблиц некоторых популярных редакторов.
Комбинированные сетевые макровирусы не только заражают создаваемые документы, но и рассылают копии этих документов по электронной почте.

По способу заражения вирусы бывают

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 вплоть до выключения или перезагрузки компьютера.

Нерезидентные

Не заражают память компьютера и являются активными ограниченное время.

По степени воздействия вирусы можно разделить на следующие виды:

- 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 алгоритмам функционирования, выделяют следующие группы:

1. Паразитические вирусы, изменяющие содержимое файлов или секторов диска; они достаточно просто могут быть обнаружены и уничтожены;

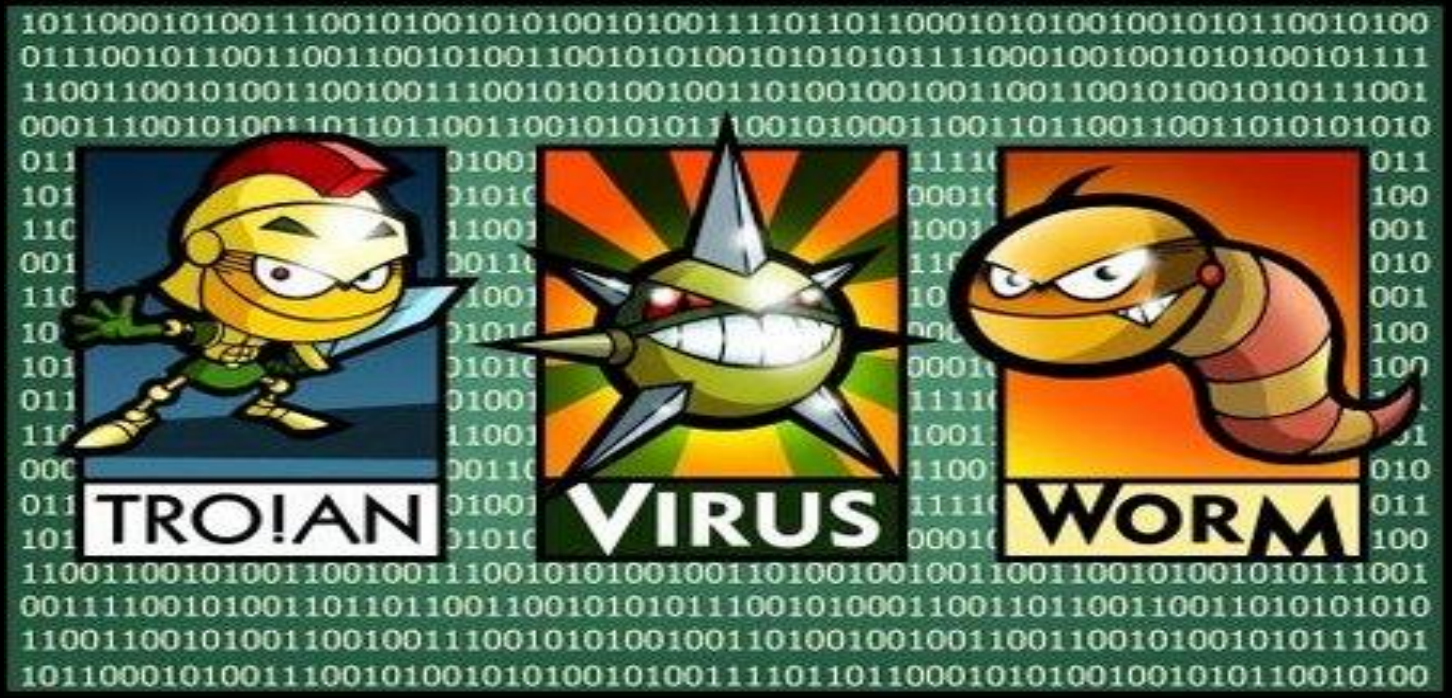
2. Вирусы-репликаторы ("черви" WORM), саморазмножающиеся и распространяющиеся по телекоммуникациям и записывающие по вычисленным адресам сетевых компьютеров транспортируемые ими опасные вирусы (сами "черви" деструктивных действий не выполняют, поэтому их часто называют псевдовирусами);

3. "Троянские" - вирусы маскируются под полезные программы (существуют в виде самостоятельных программ, имеющих то же имя, что и действительно полезный файл, но иное расширение имени; часто, например, присваивают себе расширение .com вместо .exe) и выполняют деструктивные функции (например, очищают файловые структуры); самостоятельно размножаться, как правило, не могут;

4. Вирусы-невидимки (стелс-вирусы), по имени самолета-невидимки "stealth", способны прятаться при попытках их обнаружения; они перехватывают запрос антивирусной программы и мгновенно либо удаляют временно свое тело из зараженного файла, либо подставляют вместо своего тела незараженные участки файлов;

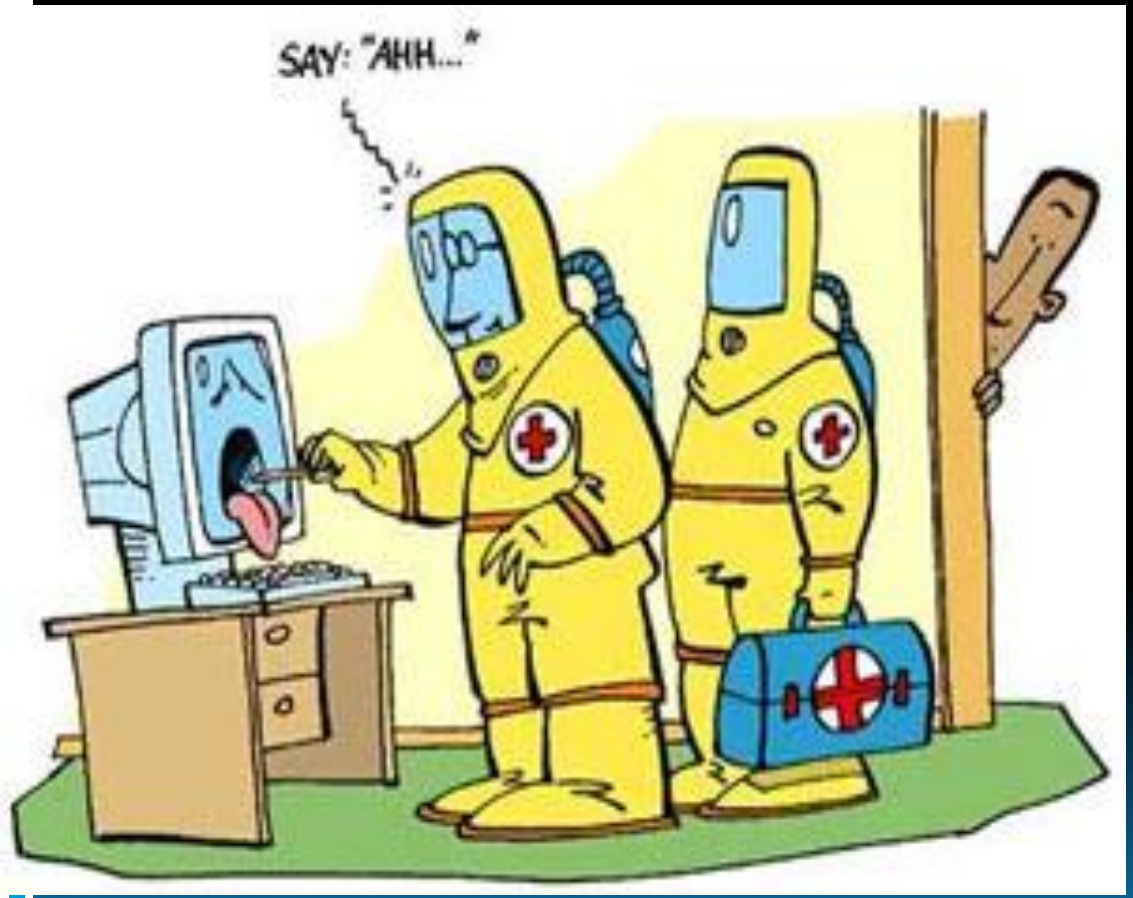
5. Самошифрующиеся вирусы (в режиме простоя зашифрованы, и расшифровываются только в момент начала работы вируса);

6. Мутирующиеся вирусы (периодически автоматически видоизменяются, копии вируса не имеют ни одной повторяющейся цепочки байт), необходимо каждый раз создавать новые антивирусные программы для обезвреживания этих вирусов;



7. «Отдыхающие" вирусы (основное время проводят в латентном состоянии и активизируются только при определенных условиях, например, вирус "Чернобыль" в сети Интернет функционирует только в день годовщины чернобыльской трагедии).

Методы защиты от компьютерных вирусов



Каким бы не был вирус, пользователю необходимо знать основные методы защиты от компьютерных вирусов.

Для защиты от вирусов можно использовать:

- общие средства защиты информации, которые полезны также и как страховка от физической порчи дисков,неправильно работающих программ или ошибочных действий пользователя;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.
- общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих средств.

- копирование информации - создание копий файлов и системных областей дисков.
- разграничение доступа предотвращает несанкционированное использование информации, в частности защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

- Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их недостаточно. Необходимо и применение специализированных программ для защиты от вирусов. Эти программы можно разделить на несколько видов: детекторы, доктора (фаги), ревизоры, доктора-ревизоры, фильтры и вакцины (иммунизаторы).

Каналы распространения

- **Дискеты**

  Самый распространённый канал заражения в 1980-90 годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов.

- **Флеш-накопители (флешки)**

  В настоящее время USB-флешки заменяют дискеты и повторяют их судьбу — большое количество вирусов распространяется через съёмные накопители, включая цифровые фотоаппараты, цифровые видеокамеры, цифровые плееры (MP3-плееры), сотовые телефоны. Использование этого канала преимущественно обусловлено возможностью создания на накопителе специального файла ***autorun.inf,*** в котором можно указать программу, запускаемую Проводником Windows при открытии такого накопителя. Флешки — основной источник заражения для компьютеров, не подключённых к сети Интернет.

- **Электронная почта**

  Сейчас один из основных каналов распространения вирусов. Обычно вирусы в письмах электронной почты маскируются под безобидные вложения: картинки, документы, музыку, ссылки на сайты.

- **Системы обмена мгновенными сообщениями**

  Так же распространена рассылка ссылок на якобы фото, музыку либо программы, в действительности являющиеся вирусами, по ICQ и через другие программы мгновенного обмена сообщениями.

- **Веб-страницы**

  Возможно также заражение через страницы Интернет ввиду наличия на страницах всемирной паутины различного «активного» содержимого: скриптов, ActiveX-компоненты, Java-апплетов

- **Интернет и локальные сети (черви)**

  Черви — вид вирусов, которые проникают на компьютер-жертву без участия пользователя. Черви используют так называемые «дыры» (уязвимости) в программном обеспечении операционных систем, чтобы проникнуть на компьютер.

Основные антивирусные программы

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

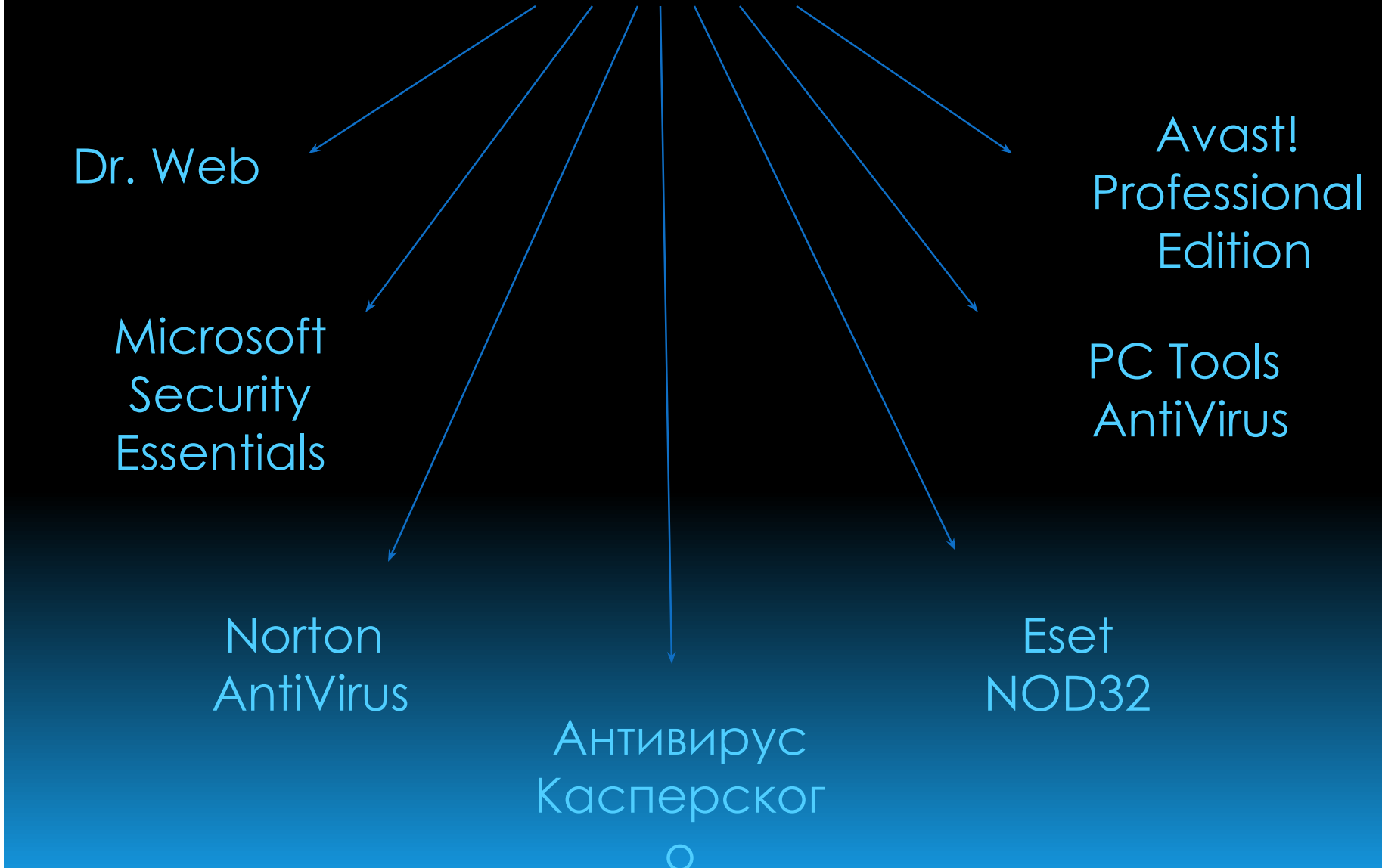
Основные виды антивирусов:

- Сканеры – основной элемент любого антивируса, осуществляет, если можно так выразиться, пассивную защиту. По запросу пользователя или заданному распорядку производит проверку файлов в выбранной области системы.

- Мониторы – в совокупности со сканерами образуют базовую защиту компьютера. На основе имеющихся сигнатур проводят проверку текущих процессов в режиме реального времени. Осуществляют предварительную проверку при попытке просмотра или запуска файла.
- Ревизоры – сохраняют в отдельную базу данные о состоянии на определенный момент критических для работы областей системы. Впоследствии сравнивает текущие файлы с зарегистрированными ранее, позволяя таким образом выявлять любые подозрительные изменения.

- Вакцины (иммунизаторы) – имитируют заражение файлов определенными вирусами. Таким образом, настоящие вирусы сталкиваются со своими «собратьями» и прекращают попытки заражения. В настоящее время данный тип программ практически не используется.

Популярные антивирусные программы



Dr. Web

Базовая защита

- Защита от вирусов, троянских программ и червей
- Защита от шпионских и рекламных программ
- Проверка файлов в автоматическом режиме и по требованию
- Проверка почтовых сообщений (перехват POP3/SMTP/IMAP)
- Проверка интернет-трафика (перехват соединений)
- Эвристическая защита от новых и неизвестных вредоносных программ
- Превентивная защита

Предотвращение угроз

- Блокирование ссылок на зараженные сайты
- Распознавание вирусов, упакованных новым и/или неизвестным упаковщиком, дроппером и/или криптором
- Dr.Web Cloud

Восстановление системы и данных

- Возможность установки программы на зараженный компьютер
- Функция самозащиты программы от выключения или остановки

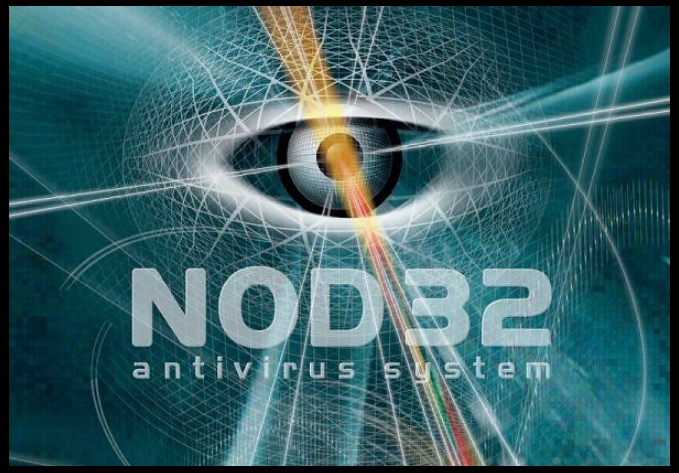
Удобство использования

- Автоматическая настройка программы в процессе установки
- Наглядное отображение результатов работы программы
- Информативные диалоговые окна для принятия пользователем обоснованных решений
- Круглосуточная техническая поддержка
- Автоматическое обновление баз

ESET NOD32 Smart Security

Надёжно

- Безопасная работа в сети интернет
- Интеллектуальная защита данных
- Безопасное общение
- Защита WI-FI
- USB-контроль
- Защита настроек
- Антиспам
- Система предотвращения вторжений (HIPS)



eset we protect your digital worlds

Быстро

- Высокая скорость
- Идеален для ноутбука
- Игровой режим
- Таймер
- Самостоятельное обновление
- Сканирование при запуске

Легко

- Понятный интерфейс
- Бесплатная техническая поддержка
- Легкий в работе

Microsoft Security Essentials

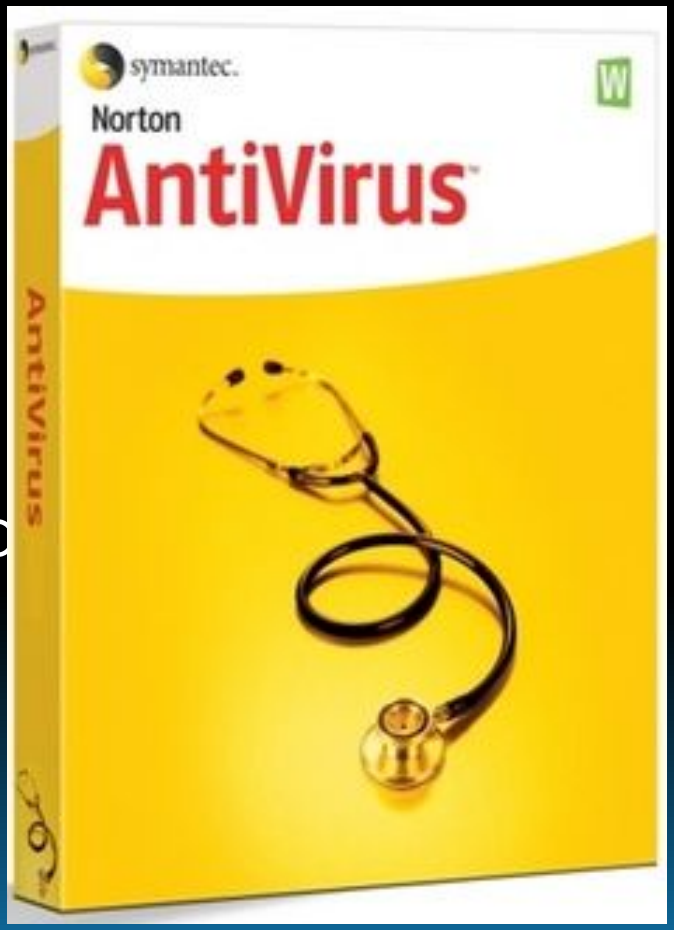
- Легкий в использовании.
- Эффективно и незаметно работает в фоновом режиме.
- Возможность обнаружения и удаления распространенных вирусов, шпионских программ, троянов, червей и других вредоносных программ.
- Технология Dynamic Signature Service.
- Защита в режиме реального времени.
- Низкое потребление системных ресурсов.
- Автоматические обновления с помощью службы Windows Update.

Microsoft®

Microsoft® Security Essentials

Norton AntiVirus

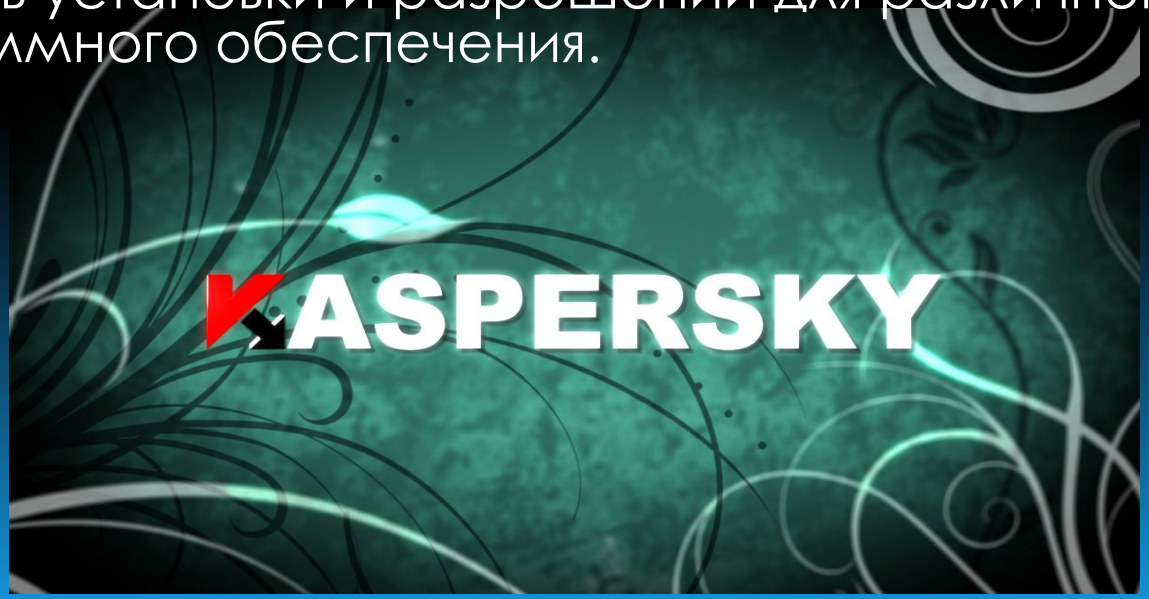
- Исключения для антивирусной защиты и SONAR
- Сканирование компьютера
- Защита в реальном времени
- Обновления
- Предотвращение вторжений
- Защита сообщений
- Параметры защиты сети
- Интеллектуальный брандмауэр
- Защита веб-браузера
- Контроль загрузок
- Identity Safe
- Безопасная работа в Интернете



Антивирус Касперского

- Особо тщательная защита в режиме реального времени.
- Глубокое сканирование файловой систем
- Также впечатляет моментальная реакция антивируса на попытки проникновения шпионских программ.
- Встроенный фаерволл позволяет не только отражать атаки вирусов, троянов, червей но и ограничивать доступ к информации, не предназначенной лицам младше 18.
- Мощный веб-экран. Блокирует все подозрительные сайты.
- Уникальная и усовершенствованная система защиты данных.
- Антивирус предназначен не только для домашнего использования, а подойдет и для защиты серверов.
- Возможность создания резервных копий и восстановления зараженных файлов.

- Регулярное и автоматическое обновление баз данных.
- Эффективная система оповещений.
- Продвинутый, но в то же время интуитивный интерфейс.
- Мощная комплексная защита от сетевых атак.
- Активный мониторинг файловой системы и контроль активности каждой программы.
- Также присутствует возможность блокирования спама и рекламы.
- Постоянное совершенствование и обновление программы.
- Предусмотрена также защита ввода с клавиатуры.
- Активно поддерживается безопасность работы в Wi-Fi сетях.
- Контроль установки и разрешений для различного программного обеспечения.



PC Tools AntiVirus

- Контроль безопасности ПК во время навигации в Интернет, а также просто во время работы и игры.
- Наличие компонента IntelliGuard, обеспечивающего защиту компьютера в режиме реального времени.
- Возможность гибкой настройки сканирования системы и параметров защиты в реальном времени.
- Возможность помещать в карантин и восстанавливать обнаруженные объекты.
- Фиксация информации обо всех сканированиях.
- Отслеживает и уничтожает (либо отправляет в карантин) попавшие на компьютер вирусы, черви и программы-шпионы.
- Постоянный контроль и обновление базы известных вирусов для обеспечения наивысшего уровня защиты.
- Скользящие подписи нового поколения, специально предназначенные для обработки огромного числа вариантов угроз.
- Система Smart Update, предназначенная для обновления дефиниций вирусов и программы в целом.

Avast! Professional Edition

- Высокий уровень выявления вирусов, троянов и червей.
- Резидентный (в режиме реального времени) и обычный сканер.
- Сканирование архивов.
- Проверка входной и выходной электронной почты.
- Глубокая интеграция в систему. Проверить тот или иной файл можно непосредственно из проводника Windows, щелкнув по нему правой кнопкой мыши и выбрав надпись "Сканировать... ".
- Карантин Avast! изолированный от операционной системы, которая обеспечивает большую безопасность работы. Ни один файл, который сохраняется в карантине не может быть запущен.
- Интуитивно понятен интерфейс Avast!. Есть русский язык.
- Большое количество настроек.
- Автоматические или запланированные обновления вирусных баз (20-80 KB). Возможность обновления "вручную".

Использованная литература:

- http://www.virustory.net/antivir.html
- http://bibliofond.ru/view.aspx?id=445550#1
- http://comp.web-3.ru/virus/?act=full&id_article=1411
- http://works.tarefer.ru/69/100023/index.html
- http://www.antivirusk.ru/2010/09/osnovnye-vidy-antivirusnyx-programm/
- https://ru.wikipedia.org/wiki/Антивирусная_программа
- http://user.pp.ua/antivirus.html
- http://modern.biblprog.org.ua/ru/pc_tools_antivirus_free

КОНЕЦ