Защита информации от вирусов.Антивирусные программы.

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

Целевые платформы антивирусного ПО:

На данный момент антивирусное программное обеспечение разрабатывается, в основном, для ОС семейства Windows от компании Microsoft, что вызвано большим количеством вредоносных программ именно под эту платформу (а это, в свою очередь, вызвано большой популярностью этой ОС, так же, как и большим количеством средств разработки, в том числе бесплатных и даже «инструкций по написанию вирусов»). В настоящий момент на рынок выходят продукты и для других операционных систем, таких, к примеру, как Linux и Mac OS X. Это вызвано началом распространения компьютерных вирусов и под эти платформы, хотя UNIX-подобные системы традиционно пользуются репутацией более устойчивых к воздействию вредоносных программ.

Помимо ОС для настольных компьютеров и ноутбуков, также существуют платформы и для мобильных устройств, такие, как Windows Mobile, Symbian, Apple iOS, BlackBerry, Android, Windows Phone 7 и др. Пользователи устройств на данных ОС также подвержены риску заражения вредоносным программным обеспечением, поэтому некоторые разработчики антивирусных программ выпускают продукты и для таких устройств.

Классификация антивирусных продуктов.

Классифицировать антивирусные продукты можно сразу по нескольким признакам, таким, как: используемые технологии антивирусной защиты, функционал продуктов, целевые платформы.

По используемым технологиям антивирусной защиты:

- Классические антивирусные продукты (продукты, применяющие только сигнатурный метод детектирования)
- Продукты проактивной антивирусной защиты (продукты, применяющие только проактивные технологии антивирусной защиты);
- Комбинированные продукты (продукты, применяющие как классические, сигнатурные методы защиты, так и проактивные)

По функционалу продуктов:

- Антивирусные продукты (продукты, обеспечивающие только антивирусную защиту)
- Комбинированные продукты (продукты, обеспечивающие не только защиту от вредоносных программ, но и фильтрацию спама, шифрование и резервное копирование данных и другие функции)

По целевым платформам:

- Антивирусные продукты для ОС семейства Windows
- Антивирусные продукты для ОС семейства *NIX (к данному семейству относятся ОС BSD, Linux и др.)
- Антивирусные продукты для ОС семейства MacOS
- Антивирусные продукты для мобильных платформ (Windows Mobile, Symbian, iOS, BlackBerry, Android, Windows Phone 7 и др.)

Антивирусные продукты для корпоративных пользователей можно также классифицировать по объектам защиты:

- Антивирусные продукты для защиты рабочих станций
- Антивирусные продукты для защиты файловых и терминальных серверов
- Антивирусные продукты для защиты почтовых и Интернет-шлюзов
- Антивирусные продукты для защиты серверов виртуализации
- и т. д.

Работа антивируса.

Говоря о системах Майкрософт, следует знать, что обычно антивирус действует по схеме:

- поиск в базе данных антивирусного ПО сигнатур вирусов
- если найден инфицированный код в памяти (оперативной и/или постоянной), запускается процесс карантина, и процесс блокируется
- зарегистрированная программа обычно удаляет вирус, незарегистрированная просит регистрации и оставляет систему уязвимой.

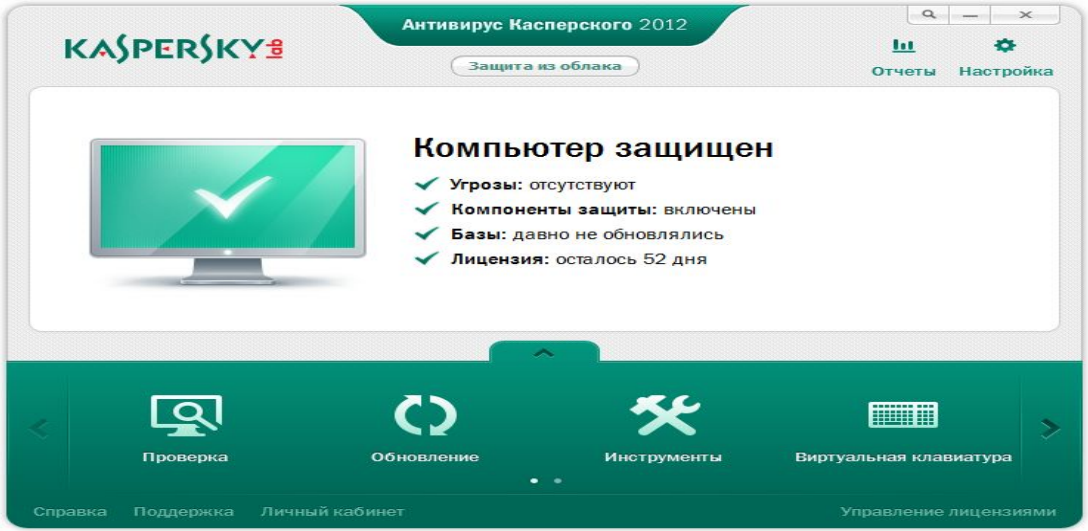
Антивирус Касперского.

Антиви́рус Каспе́рского (англ. *Kaspersky Antivirus, KAV*) — антивирусное программное обеспечение, разрабатываемоеЛабораторией Касперского. Предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, руткитов, adware, а также неизвестных угроз с помощью проактивной защиты, включающей компонент HIPS(только для старших версий, именуемых «Kaspersky Internet Security 2009+, где '+' — порядковый номер предыдущего регистра, ежегодно увеличиваемый на единицу в соответствии с номером года, следующим за годом выпуска очередной версии антивируса»). Первоначально, в начале 1990-х, именовался **-V**, затем — **AntiViral Toolkit Pro**.

Кроме собственно антивируса,

также выпускается бесплатная лечащая

утилита Kaspersky Virus Removal Tool.



Функции:

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 (для любых почтовых клиентов)
- Проверка интернет-трафика (для любых интернет-браузеров)
- Защита интернет-пейджеров (ICQ, MSN)
- Проактивная защита от новых вредоносных программ
- Проверка Java- и Visual Basic-скриптов
- Защита от скрытых битых ссылок
- Постоянная проверка файлов в автономном режиме
- Постоянная защита от фишинговых сайтов

Предотвращение угроз

- Поиск уязвимостей в ОС и установленном ПО
- Анализ и устранение уязвимостей в браузере Internet Explorer
- Блокирование ссылок на зараженные сайты
- Распознавание вирусов по способу их упаковки
- Глобальный мониторинг угроз (Kaspersky Security Network)

Восстановление системы и данных

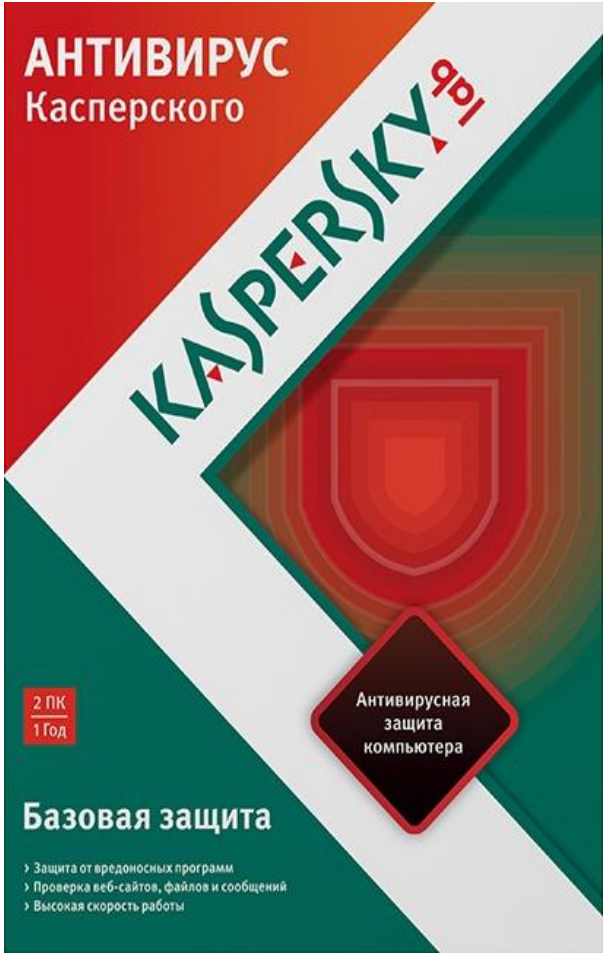
- Возможность установки программы на зараженный компьютер
- Функция самозащиты программы от выключения или остановки
- Восстановление корректных настроек системы после удаления вредоносного ПО
- Наличие инструментов для создания диска аварийного восстановления

Защита конфиденциальных данных

- Блокирование ссылок на фишинговые сайты
- Защита от всех видов кейлоггеров

Удобство использования

- Автоматическая настройка программы в процессе установки
- Готовые решения (для типичных проблем)
- Наглядное отображение результатов работы программы
- Информативные диалоговые окна для принятия пользователем обоснованных решений
- Возможность выбора между простым (автоматическим) и интерактивным режимами работы
- Круглосуточная техническая поддержка
- Автоматическое обновление баз



Общие требования для всех операционных систем

Около 480 Мб свободного пространства на жестком диске (в зависимости от размера антивирусных баз)

CD-ROM для установки программы с диска

Компьютерная мышь

Подключение к интернету для активации продукта и получения регулярных обновлений

Microsoft Internet Explorer 6.0 или выше

Microsoft Windows Installer 2.0 или выше

Dr.Web

Dr. Web (рус. ***Доктор Веб***) — 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.
Разрабатывается компанией Доктор Веб.

Характерные особенности Dr.Web

Возможность установки на зараженную машину. Начиная с версии 8.0, установка производится новым защищенныминсталлятором, который противодействует всем видам вредоносного ПО, что позволяет корректно установить антивирус на зараженную систему. В процессе установки производится обновление вирусных баз и компонентов антивируса.

Origins Tracing — алгоритм несигнатурного обнаружения вредоносных объектов, который дополняет традиционные сигнатурный поиск и эвристический анализатор, дает возможность значительно повысить уровень детектирования ранее неизвестных вредоносных программ. Также используется в *Dr.Web для Android*

Подсистема *Anti-rootkit API* (*ArkAPI*), использующая универсальные алгоритмы нейтрализации угроз. Посредством этой системы происходит нейтрализация угроз всеми компонентами антивируса. Так же используется в лечащей утилите Dr.Web CureIt! 8.0

Dr. Web Shield — механизм борьбы с руткитами, реализованный в виде драйвера. Обеспечивает низкоуровневый доступ к вирусным объектам, скрывающимся в глубинах операционной системы.

Fly-code — эмулятор с динамической трансляцией кода, реализующий механизм универсальной распаковки вирусов, защищённых от анализа и детектирования одним или цепочкой новых и/или неизвестных упаковщиков, крипторов и дропперов. Это позволяет распаковывать файлы, защищенные, к примеру, ASProtect, EXECryptor, VMProtect и тысячами других упаковщиков и протекторов, включая неизвестные антивирусу.

Поддержка большинства существующих форматов упакованных файлов и архивов, в том числе многотомных и самораспаковывающихся архивов.

Обновления вирусных баз производятся немедленно по мере выявления новых вирусов, до нескольких раз в час. Разработчики антивирусного продукта отказались от выпуска обновлений вирусных баз по какому-либо графику, поскольку вирусные эпидемии не подчиняются таковым.

Модуль самозащиты *SelfPROtect*, защищающий компоненты антивируса (файлы, ключи реестра, процессы и т.д.) от изменения и удаления вредоносным ПО.

Background Rootkit Scan - подсистема фонового сканирования и нейтрализации активных угроз. Данная подсистема находится в памяти в резидентном состоянии и осуществляет сканирование системы на предмет активных угроз и их нейтрализацию в различных областях, например: объекты автозагрузки, запущенные процессы и модули, системные объекты, оперативная память, MBR/VBR[en] дисков, системный BIOS компьютера.

Dr.Web Cloud — сервис облачной проверки ссылок в реальном времени на серверах компании «Доктор Веб», позволяющий антивирусу использовать наиболее свежую информацию о небезопасных ресурсах.

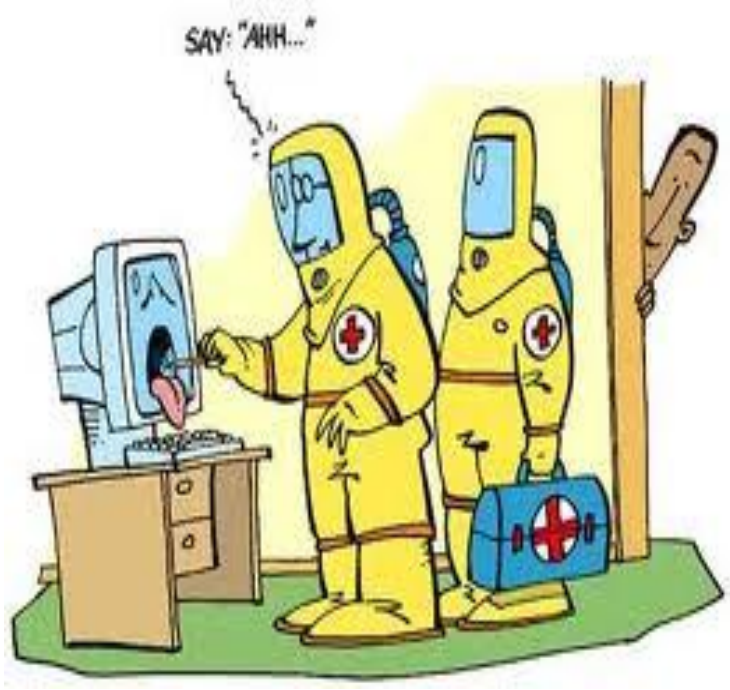
Кроссплатформенность — используется единая вирусная база и единое ядро антивирусного сканера на разных платформах ОС.

Обнаружение и лечение сложных полиморфных, шифрованных вирусов и руткитов.

Функции

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



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