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

Компьютерные вирусы. Антивирусные программы

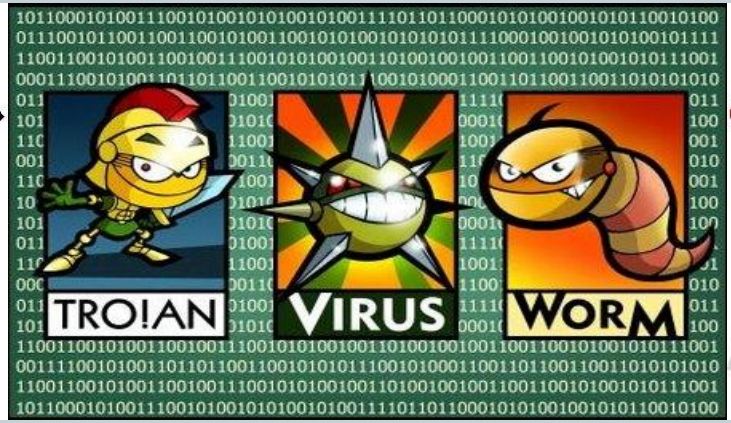
Автор: Воробьёва Виктория, 10 класс,
Руководитель: Александрова З.В., учитель
МБОУ СОШ №5 пгт Печенга, Мурманская обл.

Цель работы:

- Рассмотреть разные виды компьютерных вирусов и найти лучшие способы защиты от них

Содержание

- Определение компьютерного вируса
- История происхождения компьютерного вируса
- Проникновение вируса в компьютер
- Симптомы заражения компьютеров
- Антивирусные программы



Определение компьютерного вируса

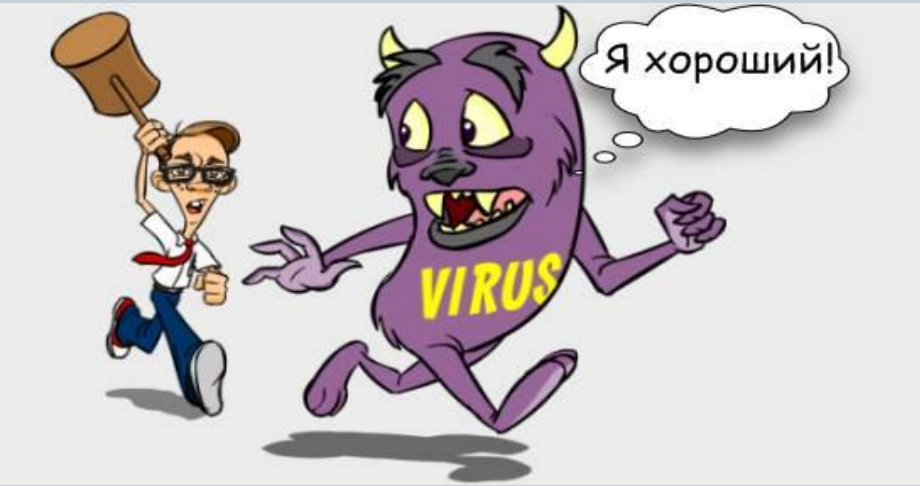
- **Компьютерный вирус** — вид вредоносного программного обеспечения, способного создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по разнообразным каналам связи.


Компьютерные вирусы могут существовать в системе в разных стадиях функционирования:

- 1. **Латентная стадия**. На этой стадии код вируса находится в системе, но никаких действий не предпринимает. Для пользователя не заметен. Может быть вычислен сканированием файловой системы и самих файлов.
- 2. **Инкубационная стадия**. На этой стадии код вируса активируется и начинает создавать свои копии, распространяя их по устройствам хранения данных компьютера, локальным и глобальным компьютерным сетям, рассылая в виде почтовых сообщений и так далее. Для пользователя может быть заметен, так как начинает потреблять системные ресурсы и каналы передачи данных, в результате чего компьютер может работать медленнее, загрузка информации из Интернет, почты и прочих данных может замедлятся.
- 3. **Активная стадия**. На этой стадии вирус, продолжая размножать свой код доступными ему способами, начинает деструктивные действия на которые ориентирован. Заметен пользователю, так как начинает проявляться основная функция вируса – пропадают файлы, отключаются службы, нарушается функционирование сети, происходит порча оборудования.

По среде обитания вирусы можно разделить на такие виды:

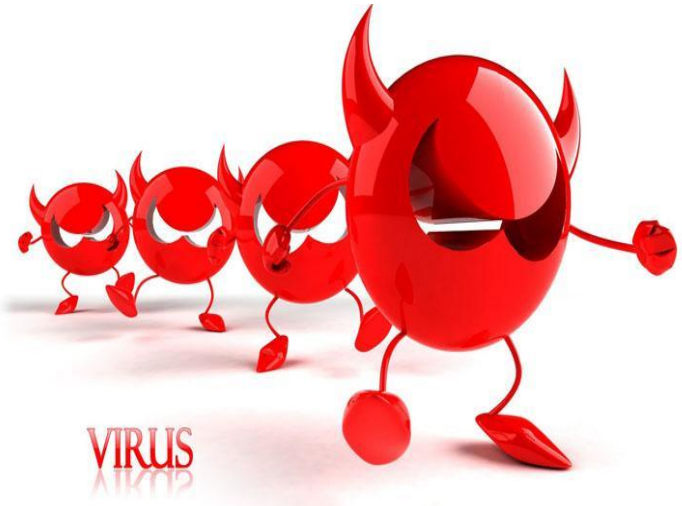
1. Загрузочные вирусы.
2. Файловые вирусы.
3. файлово-загрузочные вирусы.
4. Сетевые вирусы.
5. Документные вирусы.



История происхождения компьютерного вируса

- История этого вида вредоносных программ началась ни много ни мало – лет 40 назад. В тот самый период, конец 60-х годов, когда компьютер можно было встретить на страницах фантастических рассказов. Тогда впервые были обнаружены программы с необычным поведением. Произошло это в небольшом числе компьютеров, принадлежавших крупным исследовательским центрам США. В отличие от нормальных программ полностью выполнявших указания человека, эти не подчинялись никаким командам. Занимались внутри компьютера непонятными делами, в результате чего сильно замедлялась работа системы.
- Но, длилось это недолго… Уже в 70-х годах появились первые настоящие вирусы, способные к размножению и даже получившие свои собственные имена: компьютер UNIVAC 1108 был заражён вирусом Pervading Animal, а компьютеры семейства IBM – 360/370 были атакованы вирусом Christmas tree.

К 1980-м число активных вирусов изменялось уже сотнями. А появление и распространение PC вызвало настоящую эпидемию – вирусы стали исчислять тысячами. Однако, термин ”компьютерный вирус” впервые был использован сотрудником Лехайского университета США Ф. Коэном на конференции по информационной безопасности в 1984 году. Первые “персональные” вирусы были довольно простыми и особо от пользователя не скрывались, “скрашивали” своё разрушительное действие (удаление файлов, разрушение логической структуры диска) выводимыми на экран картинками и каверзными “шутками”: “Назовите точную высоту горы Килиманджаро в миллиметрах! При введении неправильного ответа все данные на вашем винчестере будут уничтожены!!!”.



Первые компьютерные вирусы

- Забавно, что первые вирусы этого типа были созданы для борьбы с пиратами: в 1985 году десятки тысяч компьютеров были заражены вирусом Brain, разработанным братьями-пакистанцами Алви. Хитрые братья Алви, владевшие собственным программным бизнесом умышленно снабжали свою продукцию вредоносной начинкой, которая срабатывала лишь при установке на компьютер нелегальной копии. За десять лет, прошедших с момента возникновения “пакистанского” вируса, его потомки смогли распространится по всему миру. Опасность этих вирусов заключалась в способности укрыться в абсолютно любой программе – в её главном, исполняемом файле. Чтобы вирус проник на компьютер и в дальнейшем начал заражать файлы с расширениями com и exe достаточно было одного единственного запуска программы.


- “Золотой век” классических вирусов продолжался около десяти лет. Сегодня их численность резко сократилась и, согласно оценкам лаборатории Касперского, составляет несколько процентов от всего вирусного поголовья. Любой современный антивирус вполне успешно может противостоять таким вирусам, да и сама операционная система неплохо защищена от их атак. Сегодня некоторые типы вирусов почти полностью истреблены. Одним из них является boot-вирус, поражающий загрузочный сектор жёстокого диска. И когда наконец-то смогли противостоять stealth-вирусам, компьютерный мир вздохнул с облегчением.

- Если на вашем компьютере ещё нет антивируса, будьте уверены - вирусы у вас точно есть!

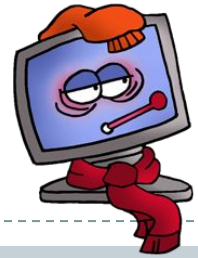
Проникновение вируса в компьютер

- Основными путями проникновения вирусов в компьютер являются съемные диски (гибкие и лазерные), а также компьютерные сети. Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Такое заражение может быть и случайным, например, если дискету не вынули из дисковода Л и перезагрузили компьютер, при этом дискета может быть к не системной. Заразить дискету гораздо проще. На нее Вирус может попасть, даже если дискету просто вставили в дисковод зараженного компьютера и, например, прочитали ее оглавление.

Проникновение вируса в компьютер

- Вирус, как правило, внедряется в рабочую программу таким образом, чтобы при ее запуске управление сначала передалось ему и только после выполнения все> ?го команд снова вернулось к рабочей программе. Получив доступ к управлению, вирус прежде всего переписывает сам себя в другую рабочую программу и заражает ее. После запуска программы, содержащей вирус, становится возможным заражение других файлов. Наиболее часто вирусом заражаются загрузочный сектор диска и исполняемые файлы, имеющие расширения EXK, COM, SYS, BAT. Крайне редко заражаются текстовые файлы.

- После заражения программы вирус может выполнить какую-нибудь диверсию (не слишком серьезную, чтобы не привлечь вниманий). И не забывает возвратить управление той программе, из которой был запущен. Каждое выполнение зараженной программы переносит вирус в следующую. Таким образом заразится асе программное обеспечение.



Симптомы заражения компьютеров

Существует ряд признаков, свидетельствующих о заражении компьютера. Если вы замечаете, что с компьютером происходят "странные" вещи, а именно:

- на экран выводятся непредусмотренные сообщения, изображения и звуковые сигналы;
- неожиданно открывается и закрывается лоток CD-ROM-устройства;
- произвольно, без Вашего участия, на вашем компьютере запускаются какие-либо программы;
- на экран выводятся предупреждения о попытке какой-либо из программ вашего компьютера выйти в интернет, хотя Вы никак не инициировали такое ее поведение,

то, с большой степенью вероятности, можно предположить, что ваш компьютер поражен вирусом.

Профилактические меры

- Не использовать сомнительные диски и другие носители информации
- Ограничить доступ к файлам программ, устанавливая для них, когда возможно, статус «только для чтения»
- При работе в сети, по возможности, не вызывайте программы из памяти других компьютеров.
- Храните программы и данные в архивах на дисках и в разных подкаталогах жесткого диска.
- Не копируйте программы для собственных нужд со случайных копий.
- Обязательно иметь антивирусную программу

Антивирусные программы

Антивирусная программа (антивирус) — изначально компьютерная программа, которая предназначена для обезвреживания вирусов и различного рода вредоносного ПО, с целью сохранности данных и оптимальной работы вашего персонального компьютера.

Самыми популярными и эффективными антивирусными программами являются *антивирусные сканеры* (другие названия: доктора, фаги, полифаги). Следом за ними по эффективности и популярности следуют *CRC-сканеры* (так-же: ревизор, checksumer, integrity checker). Часто оба приведенных метода объединяются в одну универсальную антивирусную программу, что значительно повышает ее мощность. Применяются также различного типа *мониторы*(фильтры, блокировщики) и *иммунизаторы* (детекторы).

Антивирусные программы

Антивирусные программы позволяют произвести защиту, обнаружение и удаление компьютерных вирусов. Все специализированные программы для защиты от вирусов можно разделить на несколько видов:

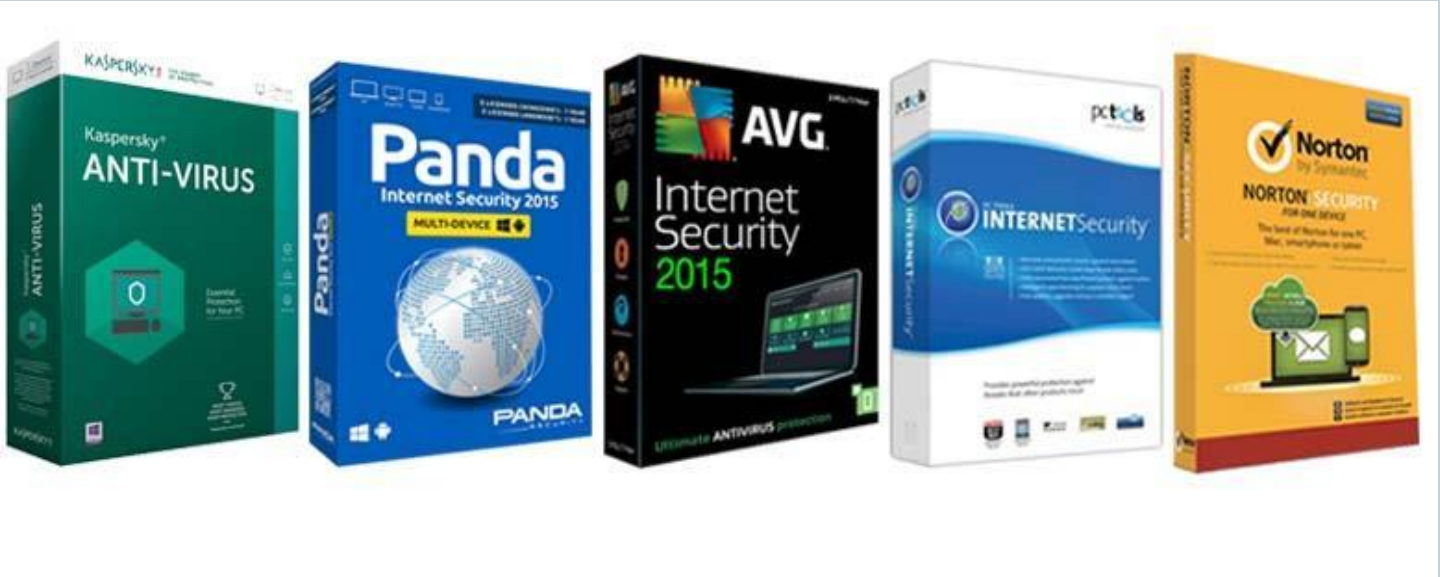
Ø детекторы,
Ø доктора (фаги),
Ø ревизоры,
Ø доктора-ревизоры,
Ø фильтры и вакцины (иммунизаторы).

Антивирусные программа

1. **Сканеры** — антивирусный модуль, который работает на основе сопоставления. Другими словами, антивирус ищет наличие вируса по базе сигнатур. Качество сканирования зависит от даты обновления баз данных и от эвристического анализа.
2. **Ревизорный модуль** — запоминает состояние файловой системы, что в последствии дает возможность сравнить отличия и сопоставить результаты. В случае отличия, вирус ловиться.
3. **Мониторы** — это специальный программы помощники, которые в случае выявления потенциально опасного вредоносного ПО(чаще всего встречаются EXE файлы) предлагают пользователю на выбор несколько операций, в число которых обязательно входит функция "удалить".
4. **Вакцины** — принцип действия этого модуля, может напоминать нам обычную "прививку". Другими словами, когда вирус хочет проникнуть и заразить программу, то роль вакцины заключается в том, чтоб показать вирусу, что программа уже заражена. К сожалению, в данный момент, когда количество вирусов в глобальной сети измеряется миллионами, данный способ уже устарел.

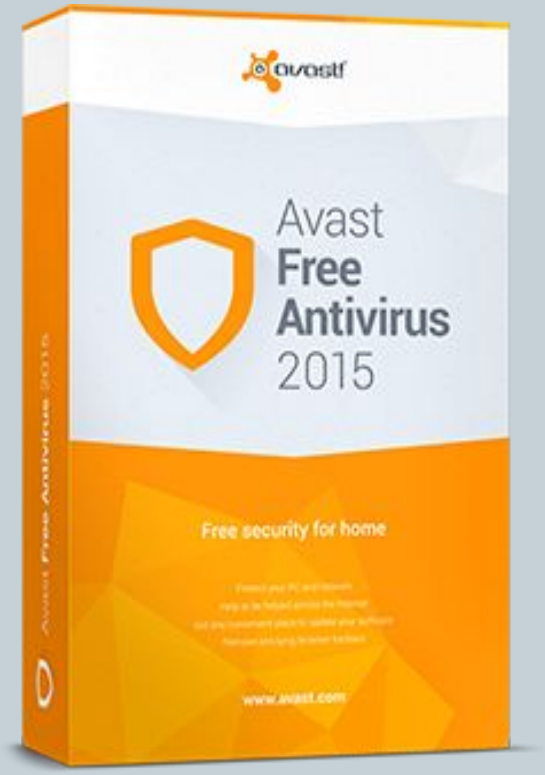
Основные задачи антивирусов

- Сканирование файлов и программ в режиме реального времени.
- Сканирование компьютера по требованию.
- Сканирование интернет-трафика.
- Сканирование электронной почты.
- Защита от атак враждебных веб-узлов.
- Восстановление поврежденных файлов (лечение).



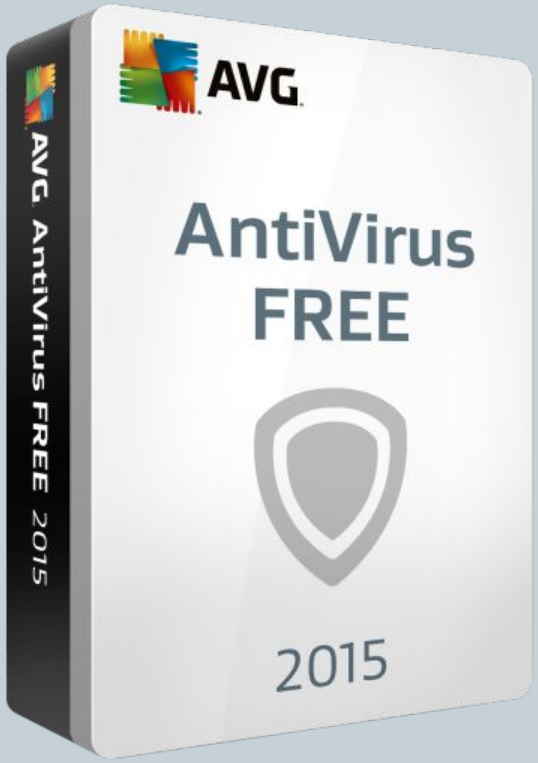
avast! Free Antivirus

- **avast! Free Antivirus — популярный бесплатный антивирус, специально разработанный для широкого использования на домашних компьютерах.** Пользователи, установившие avast! Free Antivirus, получают полную защиту от вирусов и шпионских программ в режиме реального времени, а также ряд других полезных инструментов для обеспечения безопасности компьютера.
- Экраны avast! Free Antivirus, работающие в режиме реального времени, постоянно отслеживают изменения в файловой системе, трафик, электронную почту, сеть, P2P, интернет-чаты и т.д. Удобный интерфейс этого антивируса обеспечивает быстрый доступ к настройкам его параметров.



AVG AntiVirus Free

- **AVG AntiVirus Free — популярный антивирус, бесплатный для домашнего использования.** Гарантированные производителем быстрые обновления вирусной базы данных, простота использования, низкие системные требования — основные преимущества этого антивируса.
- От платной версии AVG AntiVirus Free отличает отсутствие нескольких некритических функций и прямой технической поддержки. AVG AntiVirus Free содержит инструменты сканирования компьютера, монитор в режиме реального времени, сканер электронной почты, систему автоматического обновления антивирусной базы и другие полезные компоненты.

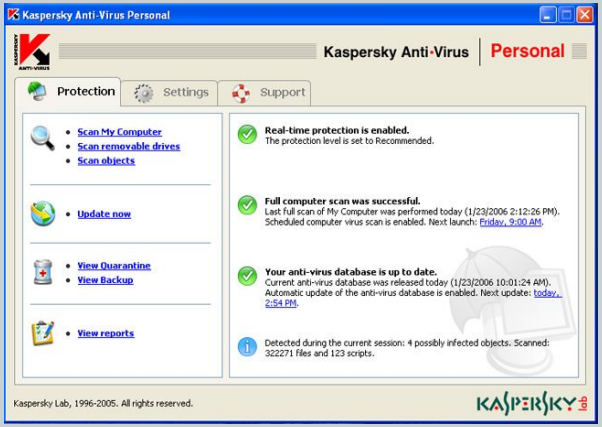


Avira Free Antivirus

- **Avira Free Antivirus — бесплатный (для частных пользователей) антивирус, предлагающий эффективную защиту против компьютерных вирусов.** Avira Free Antivirus находит и уничтожает вирусы и трояны, в том числе и еще неизвестные макровирусы. Есть возможность постоянного мониторинга системы.
- К наиболее сильным сторонам Avira Free Antivirus следует отнести хорошо отработан механизм детектирования полиморфных вирусов.

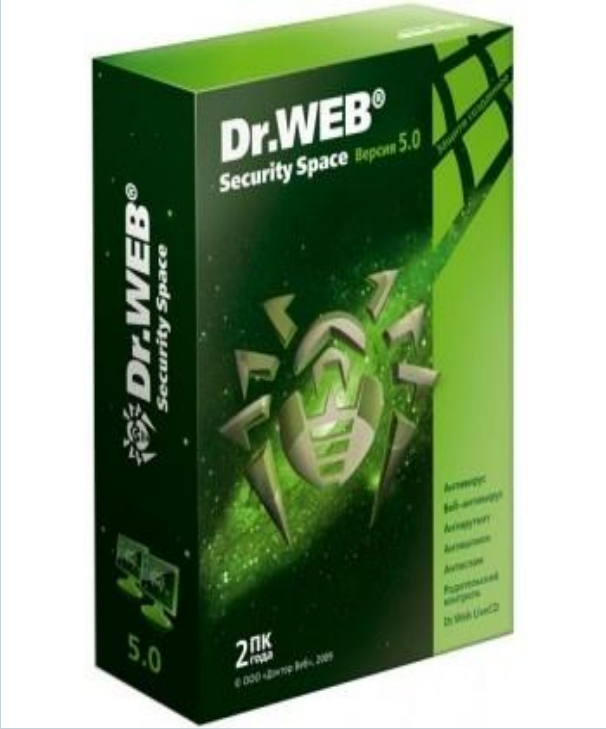
Антивирус Касперского

- **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 (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.



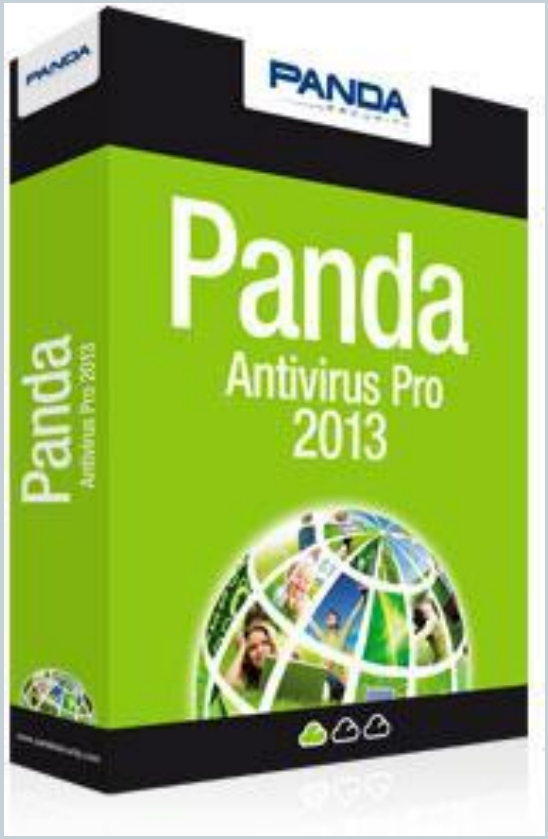
Dr.Web

- **Dr.Web** — общее название семейства программного антивирусного ПО для различных платформ (Windows, OS X, Linux, мобильные платформы) и линейки программно-аппаратных решений (Dr.Web Office Shield), а также решений для обеспечения безопасности всех узлов корпоративной сети (Dr.Web Enterprise Suite). Разрабатывается компанией «Доктор Веб».
- Продукты предоставляют защиту от вирусов, троянского, шпионского и рекламного ПО, червей, руткитов, хакерских утилит, программ-шуток, а также неизвестных угроз с помощью различных технологий реального времени и превентивной защиты.



Panda Cloud Antivirus

- **Panda Cloud Antivirus** — антивирусное программное обеспечение с функциями брандмауэра, разрабатываемое Panda Security. Продукт был представлен весной 2009 года CEO компании Хуаном Сантана в качестве защитного решения с новой моделью защиты, использующей облачные вычисления. Программа предоставляет пользователю защиту от вирусов, троянских программ, шпионских программ, червей, adware и дозвонщиков. На ноябрь 2011 года серверы «Коллективного Разума» Panda Cloud Antivirus проанализировали более 200 млн файлов.



Защитите свой компьютер от вирусов!