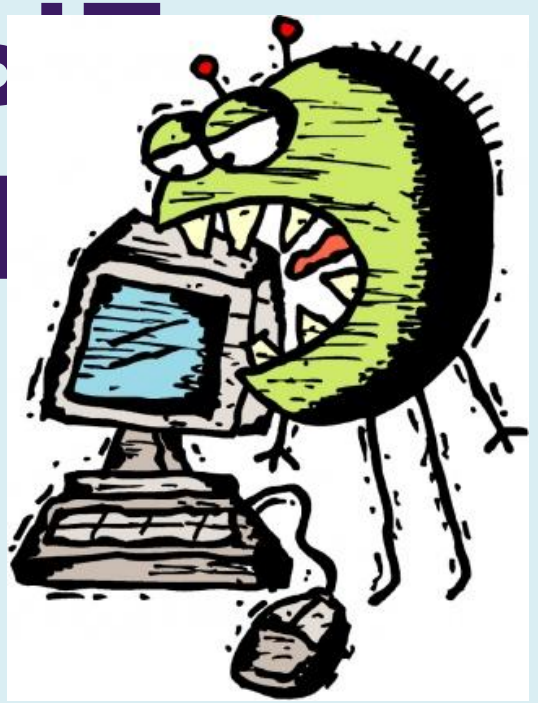
КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНЫЕ ПРОГРАММЫ

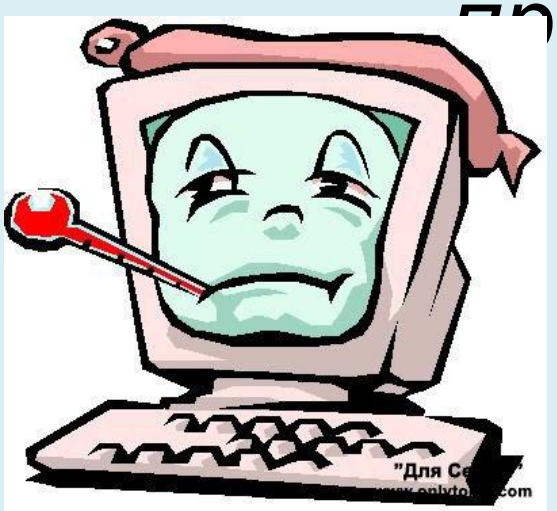


Компьютерный вирус –

это специально написанная, как правило, небольшая по размерам программа, которая может записывать (внедрять) свои копии (возможно измененные) в компьютерные программы, расположенные в исполнимых файлах, системных областях дисков, драйверах, документах и т.д., причем эти копии сохраняют возможность к «размножению».

Процесс внедрения вирусом своей копии в другую программы называется **заражением**, а программа или иной объект, содержащий вирус – **зараженным**.

Активизация компьютерного вируса может вызывать уничтожение программ и данных.



Большинство специалистов сходятся на мысли, что компьютерные вирусы, как таковые, впервые появились в 1986 году, хотя исторически возникновение вирусов тесно связано с идеей создания самовоспроизводящихся программ.

Одним из "пионеров" среди компьютерных вирусов считается вирус "Brain", созданный пакистанским программистом по фамилии Алви. Только в США этот вирус поразил свыше 18 тыс. компьютеров.

В настоящее время известно более пятидесяти тысяч вирусов, заражающих компьютеры с различными операционными системами и распространяющихся по компьютерным сетям.

ОСНОВНЫЕ ИСТОЧНИКИ ВИРУСОВ:

1. Дискеты. *Самый распространённый канал заражения в 1980—1990-е годы. Сейчас практически отсутствует из-за появления более распространённых и эффективных каналов и отсутствия флоппи-дисководов на многих современных компьютерах.*
2. Флеш-накопители *(цифровые фотоаппараты, цифровые видеокамеры, портативные цифровые плееры, мобильные телефоны)*
3. Электронная почта
4. Системы обмена мгновенными сообщениями.
5. Веб-страницы.
6. Жесткий диск, на который попал вирус в результате работы с зараженными программами;
7. Вирус, оставшийся в оперативной памяти после предшествующего пользователя

ОСНОВНЫЕ РАННИЕ ПРИЗНАКИ ЗАРАЖЕНИЯ КОМПЬЮТЕРА ВИРУСОМ:

- уменьшение объема свободной оперативной памяти;
- замедление загрузки и работы компьютера;
- непонятные (без причин) изменения в файлах, а также изменения размеров и даты последней модификации файлов;
- ошибки при загрузке операционной системы;
- невозможность сохранять файлы в нужных каталогах;
- непонятные системные сообщения, музыкальные и визуальные эффекты и т.д.

Признаки активной фазы вируса:

- исчезновение файлов;
- форматирование жесткого диска;
- невозможность загрузки файлов или операционной

По величине вредных воздействий вирусы можно разделить на:

- **неопасные,** влияние которых ограничивается уменьшением свободной памяти на диске, графическими, звуковыми и другими внешними эффектами;
- **опасные,** которые могут привести к сбоям и зависаниям при работе компьютера;
- **очень опасные**, активизация которых может привести к потере программ и данных (изменению или удалению файлов и каталогов), форматированию винчестера и так далее.

ПРИНЯТО РАЗДЕЛЯТЬ ВИРУСЫ:

- **по поражаемым объектам** на поражаемым **операционным системам и платформам** (DOS, Microsoft Windows, Unix, Linux);
- **по технологиям, используемым вирусом** (полиморфные вирусы, стелс-вирусы, руткиты);
- **по языку, на котором написан вирус** (ассемблер, высокоуровневый язык программирования, скриптовый язык и др.);
- **по дополнительной вредоносной функциональности** (бэкдоры, кейлоггеры, шпионы, ботнеты и др.).

ПО СРЕДЕ ОБИТАНИЯ ВИРУСЫ БЫВАЮТ:

1) ***Загрузочные вирусы*** передаются через зараженные загрузочные сектора при загрузке ОС и внедряется в оперативную память(ОП), заражая другие файлы.

Очень опасные, могут привести к полной потере всей информации, хранящейся на диске!

Правила защиты:

1)Не рекомендуется запускать файлы сомнительного источника (например, перед загрузкой с диска А – проверить антивирусными программами);

2) установить в BIOS ПК (Setup) защиту загрузочного сектора

2) *Файловые вирусы* способны внедряться в программы и активизируются при их запуске.

Из ОП вирусы заражают другие программные файлы (com, exe, sys) меняя их код вплоть до момента выключения ПК.

Передаются с нелегальными копиями популярных программ, особенно компьютерных игр. Но не могут заражать файлы данных (изображения, звук).

3) загрузочно-файловые вирусы способные поражать как код boot-секторов, так и код файлов;

4) *Макровирусы* - заражают файлы данных (документов Office, Autocad и др.).

Эти вирусы являются фактически макрокомандами (макросами) и встраиваются в документ, заражая стандартный шаблон документов. Угроза заражения прекращается после закрытия приложения.

При открытии документа в приложениях Word и Excel сообщается о присутствии в них макросов и предлагается запретить их загрузку. Выбор запрета на макросы предотвратит загрузку от зараженных, но и отключит возможность использования полезных макросов в документе.

5) вирусы-невидимки или Стелс-вирусы фальсифицируют информацию прочитанную из диска так, что программа, какой предназначена эта информация получает неверные данные.

Эта технология, которую, иногда, так и называют Stealth-технологией, может использоваться как в BOOT-вирусах, так и в файловых вирусах;

6) ретровирусы заражают антивирусные программы, стараясь уничтожить их или

7) *Сетевые вирусы* – распространяются по компьютерной сети посредством сетевых служб и протоколов. (рассылка почты, доступ к файлам по FTP, доступ файлам через службы локальных сетей)

Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. Полноценные компьютерные вирусы при этом обладают возможностью запустить на удаленном компьютере свой код на выполнение.

- **Троянские программы**— имитируют какие-либо полезные программы, новые версии популярных утилит или дополнений к ним. При их записи пользователем на свой компьютер троянские программы активизируются и выполняют нежелательные действия.
- **утилиты скрытого администрирования.** Они самостоятельно устанавливают на компьютере систему скрытого удаленного управления. В результате возникает возможность скрытого управления этим компьютером. Реализуя заложенные алгоритмы, утилиты без ведома пользователя принимают, запускают или отсылают файлы, уничтожают информацию, перезагружают компьютер и т. д. Возможно использование этих утилит для обнаружения и передачи паролей и ной конфиденциальной информации, запуска вирусов, уничтожения данных

Троянские программы:

1. **Логические бомбы (временные)**

   - удаляющие/модифицирующие) информацию в определенное время либо по условию.

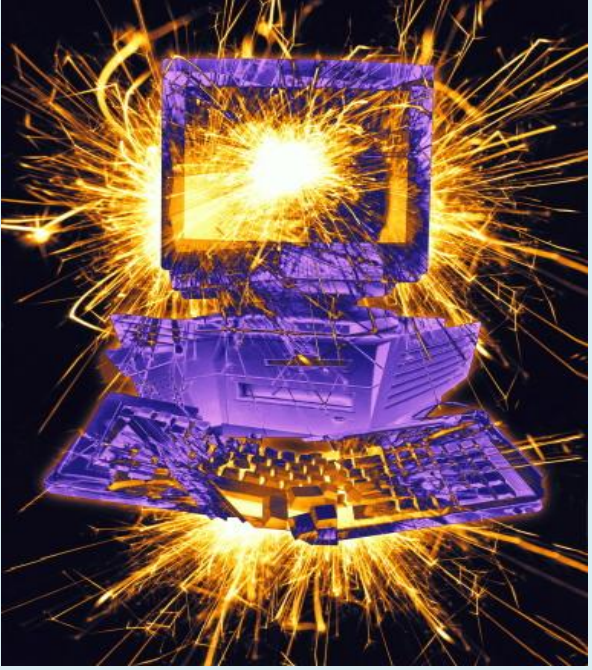
2. **Шпионы** – *собирающие информацию и складирующие ее или отправляющие данные по эл. почте*

3. **Back Door программы** – *удаленное управление компьютером или получение команд от злоумышленников*

ПРОФИЛАКТИКА И ЛЕЧЕНИЕ

В настоящий момент существует множество антивирусных программ, используемых для предотвращения попадания вирусов в ПК. Однако нет гарантии, что они смогут справиться с новейшими разработками. Поэтому следует придерживаться некоторых мер предосторожности, в частности:

- Не работать под привилегированными учётными записями без крайней необходимости.
- Не запускать незнакомые программы из сомнительных источников.
- Стараться блокировать возможность несанкционированного изменения системных файлов.
- Отключать потенциально опасный функционал системы (например, autorun-носителей в MS Windows, сокрытие файлов, их расширений и пр.).
- Не заходить на подозрительные сайты, обращать внимание на адрес в адресной строке обозревателя.
- Пользоваться только доверенными дистрибутивами.
- Постоянно делать резервные копии важных данных и иметь образ системы со всеми настройками для быстрого развёртывания.
- Выполнять регулярные обновления часто используемых программ, особенно тех, которые обеспечивают безопасность системы.



АНТИВИРУСНЫЕ ПРОГРАММЫ

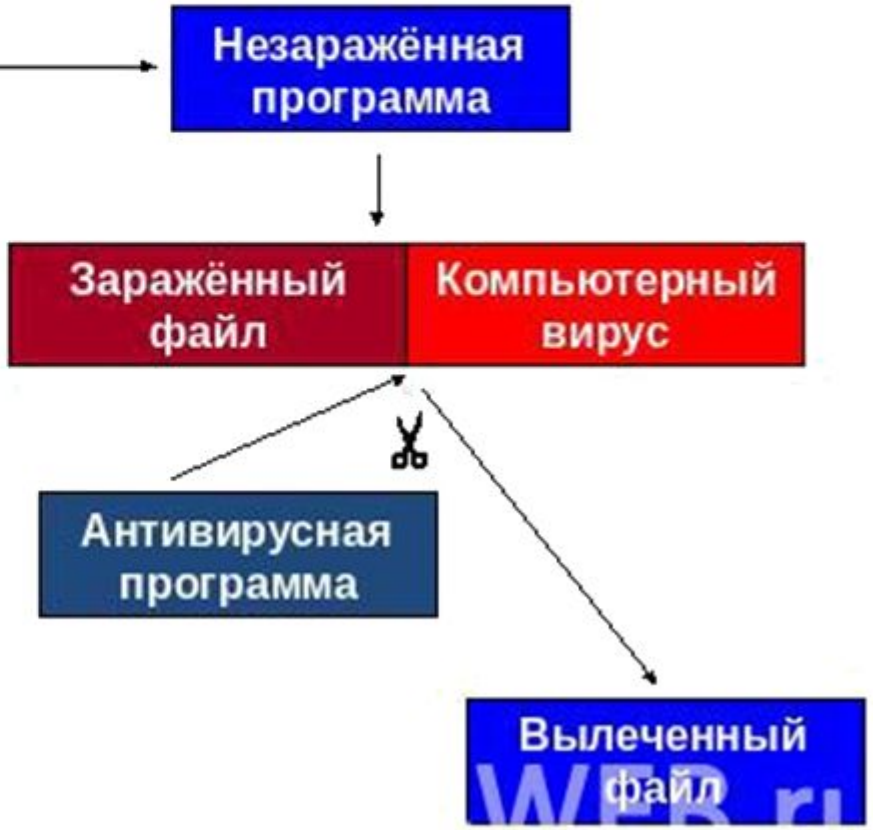
Антивирусная программа - программа, предназначенная для борьбы с компьютерными вирусами.

В своей работе эти программы используют различные принципы для поиска и лечения зараженных файлов.

Для нормальной работы на ПК каждый пользователь должен следить за обновлением антивирусов.

Если антивирусная программа обнаруживает вирус в файле, то она удаляет из него программный код вируса. Если лечение невозможно, то зараженный файл удаляется целиком.

ПРОЦЕСС ЗАРАЖЕНИЯ ВИРУСОМ И ЛЕЧЕНИЯ ФАЙЛА



ТИПЫ АНТИВИРУСНЫХ ПРОГРАММ

- *Антивирусные сканеры*
- *Детекторы(Полифаги)*
- *Антивирусные сторожа (мониторы)*
- *CRC – СКАНЕРЫ (Ревизоры)*
- *Блокировщики*

АНТИВИРУСНЫЕ СКАНЕРЫ

После запуска проверяют файлы и оперативную память и обеспечивают нейтрализацию найденного вируса.

Лечение в Kaspersky Virus Removal Tool может быть произведено автоматически или вручную

ПРОГРАММЫ-ДЕТЕКТОРЫ

проверяют, имеется ли в файлах на дисках специфическая для данного вируса комбинация байтов. При ее обнаружении выводится соответствующее сообщение.

Самые универсальные и эффективные антивирусные программы. Проверяют файлы, загрузочные сектора дисков и ОП на поиск новых и неизвестных вирусов.

Недостаток — возможность защиты только от известных вирусов. Занимают много места, работают не быстро.

NORTON ANTIVIRUS

DR WEB

AVAST

KASPERSKY ANTIVIRUS

ПРОГРАММЫ-МОНИТОРЫ (ПРОГРАММЫ-ФИЛЬТРЫ)

постоянно находятся в ОП и обеспечивают проверку файлов в процессе их загрузки в ОП, перехватывают и сообщают пользователю о обращениях ОС, которые используются вирусами для размножения и нанесения ущерба. Пользователь имеет возможность разрешить или запретить выполнение этих обращений.

К преимуществу таких программ относится возможность обнаружения неизвестных вирусов. Использование программ-фильтров позволяет обнаруживать вирусы на ранней стадии заражения компьютера.

Недостатками программ являются невозможность отслеживания вирусов, обращающихся непосредственно к BIOS, а также загрузочных вирусов, активизирующихся до запуска антивируса при загрузке DOS, и частая выдача запросов на выполнение операций.

PROCESS MONITOR

Программы - Ревизоры

Следят за изменениями файловой системы, для этого они запоминают названия файлов и папок, размеры файлов и их контрольные суммы. Периодически (по расписанию) или по приказу пользователя ревизор проверяет текущее состояние файловой системы и сравнивает с прежним. О подозрительных изменениях немедленно сообщается, об остальных пользователь может узнать при желании.

Достоинствами ревизоров как антивирусов являются:

- **Быстрота проверки.** В отличие от сканеров, которые должны содержимое файлов сверить с тысячами известных вирусных сигнатур, ревизор подсчитывает лишь контрольную сумму. Это даёт экономию времени в десятки раз.
- **Выявление любых новых вирусов.** Если вирус отсутствует в базе данных (еще не занесён в базу или у данного пользователя устаревшая база), то сканер обычно не замечает вирус. Но любой вирус изменяет систему данных на диске, следовательно, выявляется ревизором.
- **Возможность восстановления некоторых испорченных и уничтоженных файлов**, а также лечения некоторых файлов, заражённых неизвестными вирусами. Ревизоры сохраняют копии коротких файлов, наиболее важных файлов и файлов, чаще всего становящихся жертвами вирусов.

Ревизоры не в состоянии защитить компьютер от всех угроз, поэтому они обычно используются в комплексе с другими антивирусными средствами.

ADINF32

Блокировщики

- перехватывающие вирусо опасные ситуации и сообщающие об этом пользователю. К вирусо опасным относятся вызовы на открытие для записи в выполняемые файлы, запись в boot-сектора дисков или MBR винчестера, попытки программ остаться резидентно и т.д., то есть вызовы, которые характерны для вирусов в моменты из размножения.
- К достоинствам блокировщиков относится их способность обнаруживать и останавливать вирус на самой ранней стадии его размножения. К недостаткам относятся существование путей обхода защиты блокировщиков и большое количество ложных срабатываний.

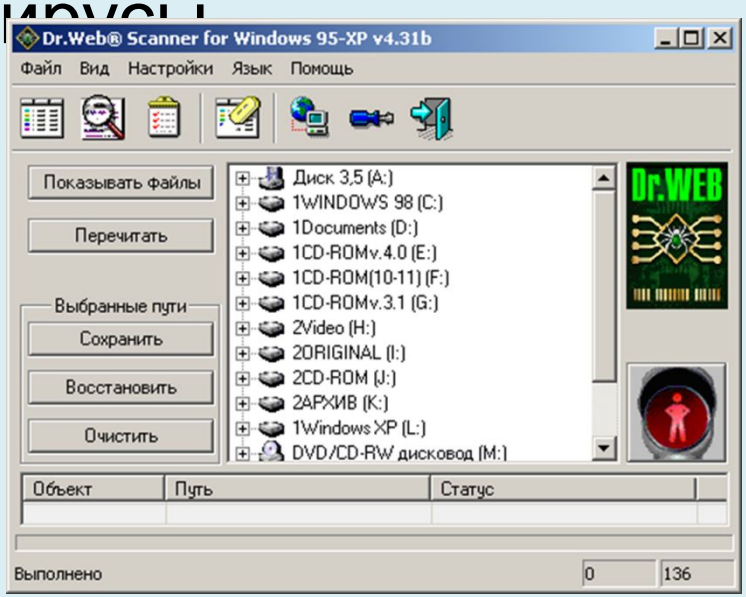
Антивирусные блокировщики могут входить в BIOS Setup.

В России наибольшее распространение получили антивирусные программы Лаборатории Касперского (Anti-IViral Toolkit Pro) и ДиалогНаука (Adinf,Dr.Web). Антивирусный пакет AntiViral Toolkit Pro (AVP) включает AVP Сканер, резидентный сторож AVP Монитор, программу администрирования установленных компонентов, Центр управления и ряд других.

AVP Сканер помимо традиционной проверки выполняемых файлов и файлов документов обрабатывает базы данных электронной почты.

DRWEB

Антивирусные программы семейства Dr.Web выполняют поиск и удаление известных программе вирусов из памяти и с дисков компьютера, а так же осуществляют эвристический анализ файлов и системных областей дисков компьютера. Эвристический анализ позволяет с высокой степенью вероятности обнаруживать новые, ранее неизвестные компьютерные вирусы.



ADINF32

Ревизор диска ADinf32 - Эта антивирусная программа фиксирует любые изменения в файловой системе компьютера и обладает удобным пользовательским интерфейсом.

Оставаясь одним из самых надежных средств обнаружения и удаления компьютерных вирусов, программа ADinf уже давно многими используется как повседневное средство контроля за состоянием информации на дисках компьютера.

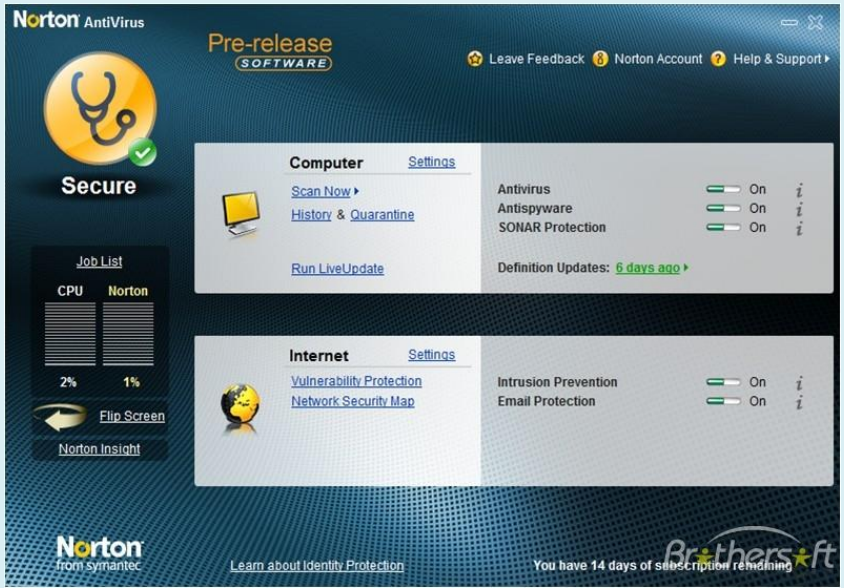
Может найти потерявшийся файл, проанализировать результаты сбоя компьютера, убедиться в сохранности баз данных и документов, найти, куда вдруг пропало все свободное место на диске, обнаружить и обезвредить компьютерный вирус.

AVAST

популярная бесплатная антивирусная программа для операционных систем Windows, Linux, Mac OS, а также для КПК на платформе Palm, Android иWindows CE. Всего же антивирусом avast! пользуются почти 200 миллионов пользователей во всём мире.

NORTON ANTIVIRUS

- Norton Antivirus является «самым-самым» сразу по целому ряду позиций. Обладатель самой большой базы данных вирусов.
- Norton Antiviras — программа на редкость «въедливая», из-под ее контроля не уйдет ни один запущенный на компьютере процесс. Включает: защиту от вирусов, защиту от программ-шпионов, защиту от руткитов, импульсные обновления и др.



АНТИВИРУС КАСПЕРСКОГО

В состав Kaspersky AntiVirus Personal Pro входят:

- Kaspersky AntiVirus Сканер,
- Kaspersky AntiVirus Монитор,
- Kaspersky AntiVirus Центр управления.

AVP Сканер имеет удобный пользовательский интерфейс, большое количество настроек, выбираемых пользователем, а также одну из самых больших в мире антивирусных баз, что гарантирует надежную защиту от огромного числа самых разнообразных вирусов: полиморфных или самошифрующихся вирусов; стелс-вирусов или вирусов-невидимок; макро вирусов, заражающих документы Word и таблицы Excel.