ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тема 5. Компьютерные вирусы

Учебные вопросы

1. **История компьютерных вирусов.**
2. **Классификация компьютерных вирусов.**
3. **Методы защиты от компьютерных вирусов.**

Введение

- **Компьютерный вирус** - это специально написанная программа, обычно небольшая по размерам, способная самостоятельно дописывать себя к другим программам (заражать их), и производить различные нежелательные действия
- Официально термин "**компьютерный вирус**" появился когда его впервые употребил сотрудник Лехайского университета (США) Ф.Коэн в **1984 г**. на 7***-й конференции по безопасности информации***, проходившей в США. С тех пор прошло немало времени, острота проблемы вирусов многократно возросла, однако строгого определения, что же такое компьютерный вирус, так и не дано, несмотря на то что многие пытались это сделать неоднократно.

- **Программа, внутри которой находится вирус, называется *«зараженной»***

Когда такая программа начинает работу, то сначала управление получает вирус.

После того, как вирус выполнит нужные ему действия, он передает управление той программе, в которой он находится, и она работает так же, как обычно.

Поэтому представляется возможным сформулировать только обязательное условие для того, чтобы некоторая последовательность выполняемого кода являлась вирусом.

Обязательное (необходимое) свойство компьютерного вируса - возможность создавать свои дубликаты (не всегда совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

1. История компьютерных вирусов

Конец 1960-х - начало 70-х годов: "***кролик***" (**the rabbit**) - программа клонировала себя, занимала системные ресурсы и таким образом снижала производительность системы.

Первая половина 70-х годов: под ОС Tenex создан вирус **The Creeper**, использовавший для своего распространения глобальные компьютерные сети. Вирус был в состоянии самостоятельно войти в сеть через модем и передать свою копию удалённой системе. Для борьбы с этим вирусом была создана программа **Reeper** – первая известная антивирусная программа.

Начало 80-х годов: компьютеры становятся всё более и более популярными, результат этого – большое число разнообразных «***троянских коней***» - программ, которые при запуске наносят системе какой-либо вред.

История компьютерных вирусов

- **1981 год**: эпидемия загрузочного вируса *Elk Cloner* на компьютерах Apple II. Вирус записывался в загрузочные сектора дискет, к которым шло обращение. Проявлял он себя весьма многосторонне – переворачивал экран, заставлял мигать текст на экране и выводил разнообразные сообщения.
- **1986 год**: эпидемия первого IBM PC-вируса *Brain*. Вирус, заражающий 360 Кб дискеты, практически мгновенно разошёлся по всему миру. Причина такого «успеха» - скорее всего, в неготовности компьютерного общества к встрече с таким явлением, как компьютерный вирус. Вирус был написан в Пакистане братьями Basit и Amjad Farooq Alvi, оставившими в вирусе текстовое сообщение, содержащее их имена, адрес и телефонный номер. Как утверждали авторы вируса, являвшиеся владельцами компании по продаже программных продуктов, они решили выяснить уровень пиратского копирования в их стране. К сожалению, их эксперимент вышел за границы Пакистана. Интересно, что этот вирус являлся также и первым «стелс»-вирусом – при попытке чтения заражённого сектора он «подставляет» его незаражённый оригинал.

История компьютерных вирусов

1987 год: появление вируса *Vienna* и ещё несколько вирусов для IBM PC. Это знаменитые в прошлом *Lehigh*, заражающий только COMMAND.COM, *Suriv-1* (другое название – April1st), заражающий COM-файлы, *Suriv-2*, заражающий (впервые) EXE-файлы, и *Suriv-3* заражающий как COM-, так и EXE-файлы. В декабре 1987 года случилась первая известная повальная эпидемия сетевого вируса *Cristmas Tree*, написанного на языке REXX и распространявшего себя в операционной среде VM/CMS. 9 декабря вирус был запущен в сеть в Западной Германии и через четыре дня 13 декабря парализовал сеть IBM Vnet. При запуске вирус выводил на экран изображение рождественской ёлочки и рассылал свои копии всем пользователям сети.

История компьютерных вирусов

- **1988 год**: в пятницу 13 мая сразу несколько фирм и университетов разных стран мира познакомились с вирусом *Jerusalem* – в этот день вирус уничтожал файлы при их запуске. Это, пожалуй, один из первых MS-DOS-вирусов, ставший причиной настоящей эпидемии: сообщения о заражённых компьютерах поступали из Европы, Америки и Ближнего Востока. Название, кстати, вирус получил по месту одного из инцидентов – университета в Иерусалиме.
- **В этом году была создана новая антивирусная программа – Dr.Solomon's Anti-Virus Toolkit, являющаяся на сегодняшний день одним из самых мощных антивирусов.**

История компьютерных вирусов

- **1989 год**: обнаружен новый вирус *Datacrime*, который имел крайне опасное проявление – с 13 октября по 31 декабря он форматировал винчестер. Следует отметить тот факт, что 1989 год являлся началом повальной эпидемии компьютерных вирусов в России – всё те же вирусы Cascade, Jerusalem, Vienna заполонили компьютеры наших соотечественников.
  В конце 1989 года в России Е.В.Касперским была разработана первая версия антивируса AVP (AntiViral Toolkit Pro).

История компьютерных вирусов

1990 год: этот год принёс несколько довольно заметных событий.

Первое из них – появление полиморфик-вирусов **Chameleon** (другое название – V2P1, V2P2, V2P6). До этого момента антивирусные программы для поиска вирусов пользовались так называемыми «масками» - кусками вирусного кода. После обнаружения вирусов Chameleon разработчики антивирусов были вынуждены искать другие методы детектирования вирусов.

Второе событие – появление болгарского «завода по производству вирусов»: огромное число новых вирусов имело болгарское происхождение. В июле произошёл инцидент с компьютерным журналом **PC Today** (Великобритания). Он содержал гибкий диск, заражённый вирусом ***DiskKiller***. Было продано более 50 000 экземпляров журнала.

История компьютерных вирусов

- **1991 год**: популяция компьютерных вирусов непрерывно растёт, достигая уже нескольких сотен. В апреле разразилась настоящая эпидемия файлово-загрузочного полиморфик-вируса ***Tequila***. Россию это событие практически не затронули.
- **Лето 1991**: эпидемия вируса ***Dir_II***, использовавшего принципиально новые способы заражения файлов (link-вирус). В целом 1991 год был достаточно спокойным – этакое затишье перед бурей, разразившейся в 1992.
- **1992 год**: первый ***полиморфик-генератор MtE***, на его базе через некоторое время появляется сразу несколько полиморфик-вирусов. Первый вирус для Windows, заражающий выполняемые файлы этой ОС, открыл новую страницу в вирусописательстве.
- **1993 год**: появляется всё больше вирусов, использующих весьма необычные способы заражения файлов, проникновения в систему и т.д.

История компьютерных вирусов

1994 год: всё большее значение приобретает проблема вирусов на CD-дисках. Быстро став популярными, эти диски и оказались одним из основных путей распространения вирусов. Зафиксировано сразу несколько инцидентов, когда вирус попадал на мастер-диск при подготовке партии CD-дисков. В результате на компьютерный рынок были выпущены довольно большие тиражи (десятки тысяч) заражённых CD-дисков. Естественно, что об их лечении говорить не приходится – их надо просто уничтожать.

В июне началась повальная эпидемия вируса OneHalf, до сих пор являющегося самым распространённым в России.

Сентябрь: «***ЗАРАЗА***» - эпидемия файлово-загрузочного вируса, использующего крайне необычный способ внедрения в MS-DOS. Ни один антивирус не оказался готовым к встрече с подобного типа монстром.

История компьютерных вирусов

1995 год: произошёл инцидент с Microsoft: на диске, содержащем демонстрационную версию Windows 95. Копии этого диска были разосланы бета-тестерами, один из которых не поленился проверить диск на вирусы.
Август: один из поворотных моментов в истории вирусов и антивирусов – в «живом виде» обнаружен первый вирус для Microsoft Word (***Concept***). Буквально за месяц вирус «облетел» весь земной шар, заполнил компьютеры пользователей MS-DOS и прочно занял первое место в статических исследованиях.

1996 год: два достаточно заметных события – появился первый вирус для Windows 95 (***Win95.Boza***) и началась эпидемия крайне сложного полиморфик –вируса ***Zhengix*** в Санкт-Питербурге.
Март: первая эпидемия вируса для Windows 3.x (***Win.Tentacle***).
Июль: ***Laroux*** - первый вирус для Microsoft Excel, к тому же пойманный в «живом виде».

История компьютерных вирусов

1997 год: макровирусы перебрались в Office 97, поэтому появились вирусы, ориентированные только на документы Office 97.

Апрель: ***Homer*** – первый сетевой вирус-червь, использующий для своего размножения File Transfer Protocol (ftp).

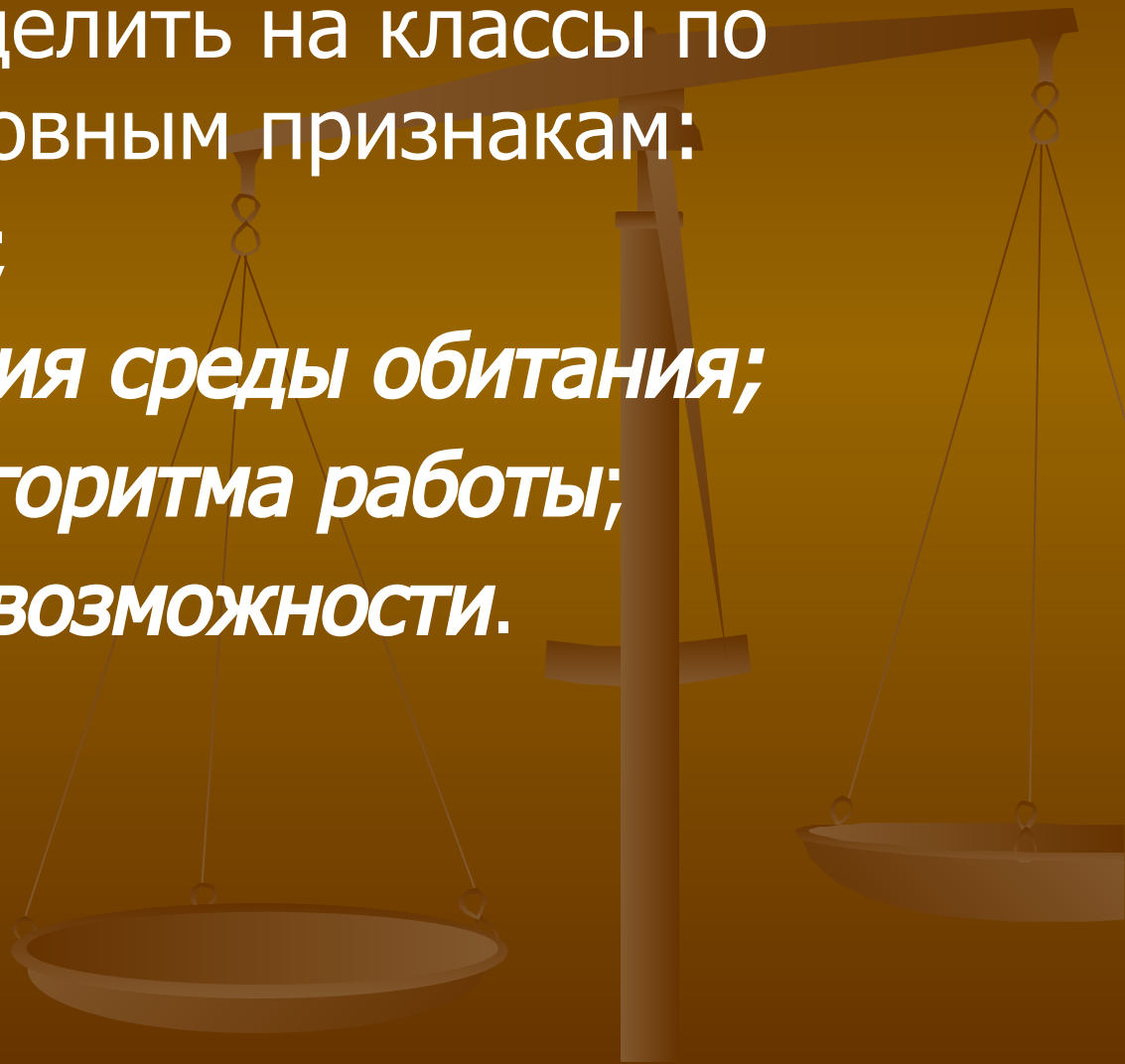
Июнь: появление первого самошифрующегося вируса для Windows 95.

2000 год: появление и эпидемия в России вируса «***I love You***».

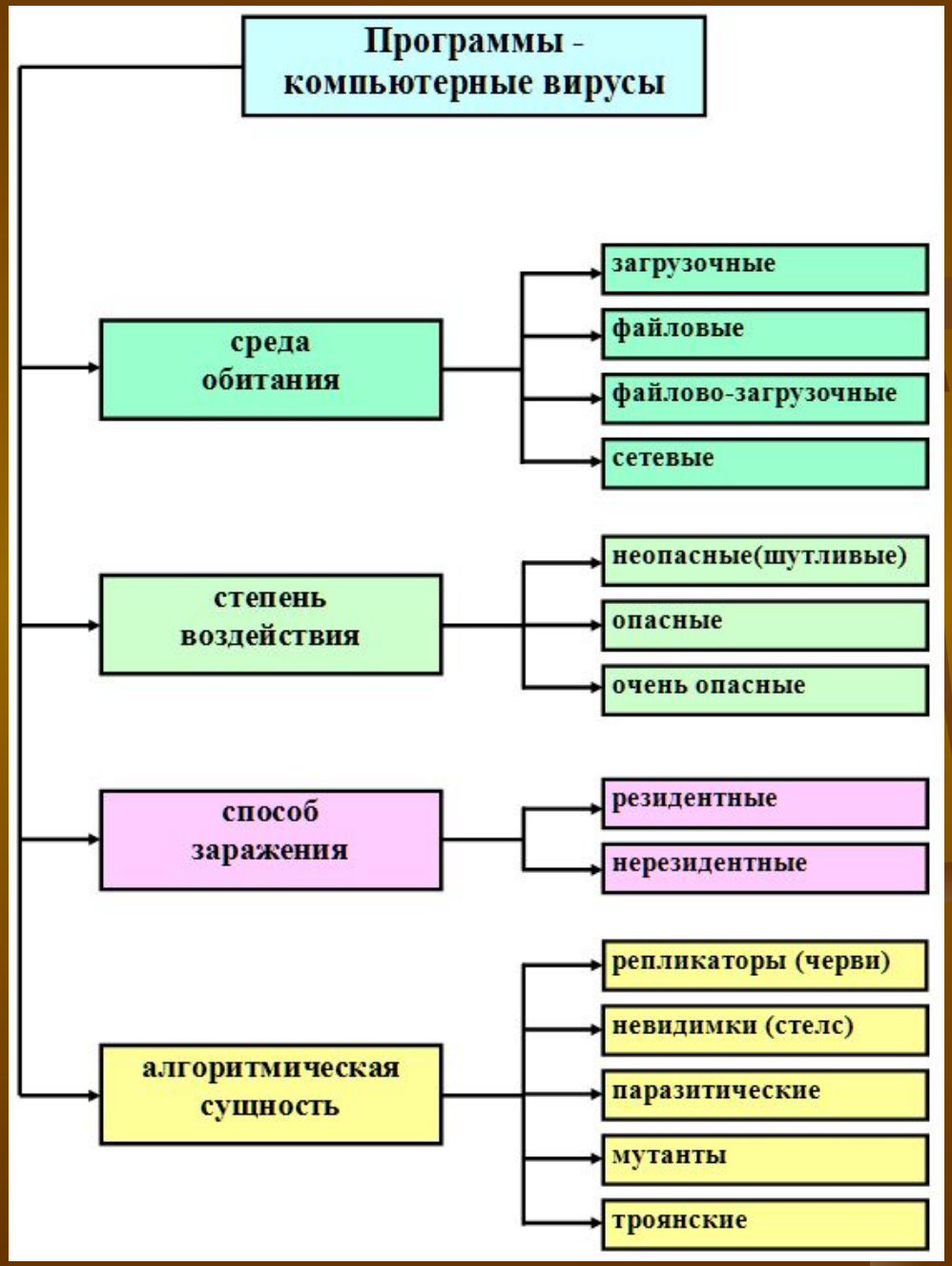
2. Классификация компьютерных вирусов:

Вирусы можно разделить на классы по следующим основным признакам:

- ***среда обитания;***
- ***способ заражения среды обитания;***
- ***особенности алгоритма работы;***
- ***деструктивные возможности.***



Классификация компьютерных вирусов



- **Файловые вирусы**
- либо различными способами внедряются в выполняемые файлы (наиболее распространённый тип вирус),
- либо создают файлы-двойники (вирусы-компаньоны),
- либо используют особенности организации файловой системы (link-вирусы).
- **Загрузочные вирусы**
- записывают себя либо в загрузочный сектор диска (boot-секторы),
- либо в сектор, содержащий системный загрузчик винчестера (Master Boot Record),
- либо меняют указатель на активный boot-сектор.
- **Макровирусы**
- заражают файлы-документы и электронные таблицы нескольких популярных редакторов.
- **Сетевые вирусы**
- используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

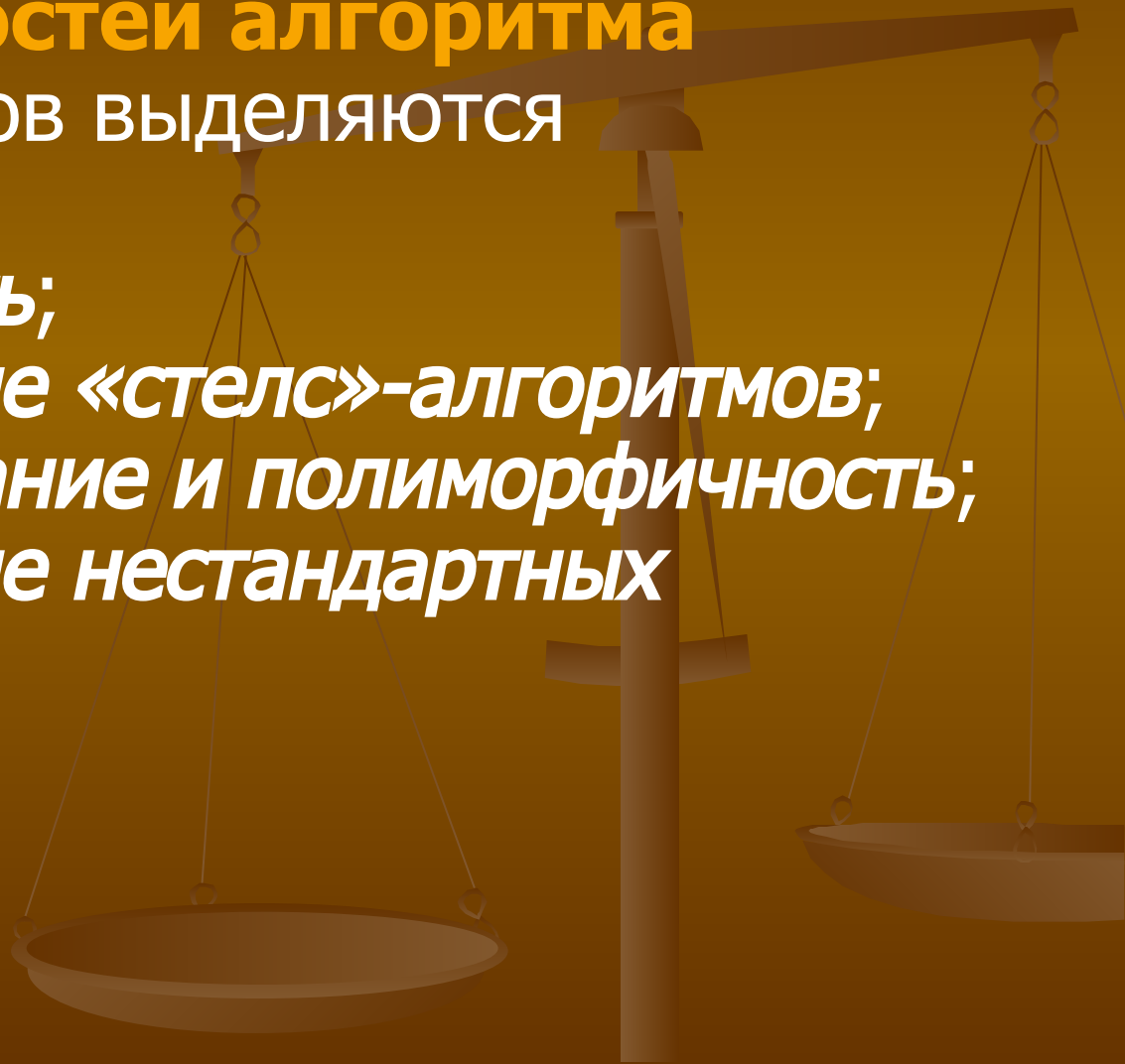
Существует большое количество сочетаний, например ***файлово-загрузочные вирусы***, заражающие как файлы, так и загрузочные секторы дисков. Такие вирусы, как правило, имеют довольно сложный алгоритм работы, часто применяют оригинальные методы проникновения в систему, используют «стелс» и полиморфик-технологии.

Другой пример такого сочетания – ***сетевой макровирус***, который не только заражает редактируемые документы, но и рассылают свои копии по электронной почте.

Заражаемая **операционная система** является вторым уровнем деления вирусов на классы. Каждый файловый или сетевой вирус заражает файлы какой-либо одной или нескольких ОС.

Среди **особенностей алгоритма работы** вирусов выделяются следующие:

- ***резидентность***;
- ***использование «стелс»-алгоритмов***;
- ***самошифрование и полиморфичность***;
- ***использование нестандартных приёмов***.



Особенности алгоритма работы вирусов

простейшие - паразитические,
они изменяют содержимое файлов и секторов диска
и могут быть достаточно легко обнаружены и уничтожены

вирусы-репликаторы - называемые *червями*, которые
распространяются по компьютерным сетям, вычисляют
адреса сетевых компьютеров и записывают
по этим адресам свои копии

вирусы-невидимки или стелс-вирусы перехватывают
обращения операционной системы к пораженным файлам и
секторам дисков и подставляют вместо своего тела
незараженные участки диска

вирусы-мутанты содержащие алгоритмы
шифровки-расшифровки,
благодаря которым копии одного и того же вируса
не имеют ни одной повторяющейся цепочки байтов;

троянские программы, маскируются под полезную программу,
разрушают загрузочный сектор и файловую систему дисков

- **Резидентный вирус**
- **Резидентный (в памяти) вирус** (Memory resident virus) - постоянно присутствующий в памяти вирус, написанный, как правило, на языке Ассемблер или Си. Такие вирусы обладают возможностью более эффективно заражать программы и противодействовать антивирусным средствам. Занимает небольшой объем памяти. Пребывает в состоянии готовности к продолжению выполнения своей задачи до выгрузки, перезагрузки или выключения компьютера. Активизируется и выполняет заданные вирусописателем действия например при достижении компьютером определенного состояния (срабатывания таймера, др.). Все бутовые вирусы резидентны.
- При инфицировании компьютера оставляет в оперативной памяти свою резидентную часть, которая затем перехватывает обращения ОС к объектам заражения и внедряется в них. Эти вирусы находятся в памяти и являются активными вплоть до выключения компьютера или перезагрузки ОС.

- Использование **«стелс»-алгоритмов** позволяет вирусам полностью или частично скрыть себя в системе. Наиболее распространённым «стелс»-алгоритмом является перехват запросов ОС на чтение-запись заражённых объектов и затем «стелс»-вирусы либо временно лечат их, либо подставляют вместо себя незаражённые участки информации.

- **Самошифрование и полиморфичность** используются практически всеми типами вирусов для того, чтобы максимально усложнить процедуру обнаружения вируса.

- Полиморфик-генераторы, как и конструкторы вирусов, не являются вирусами в прямом смысле этого слова, поскольку в их алгоритм не закладываются функции размножения, т.е. открытия, закрытия и записи в файлы, чтения и записи секторов и т.д. Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика.

- Обычно полиморфные генераторы распространяются их авторами без ограничений в виде файла-архива. Основным файлом в архиве любого генератора является объектный модуль, содержащий этот генератор. Во всех встречавшихся генераторах этот модуль содержит внешнюю (external) функцию - вызов программы генератора.

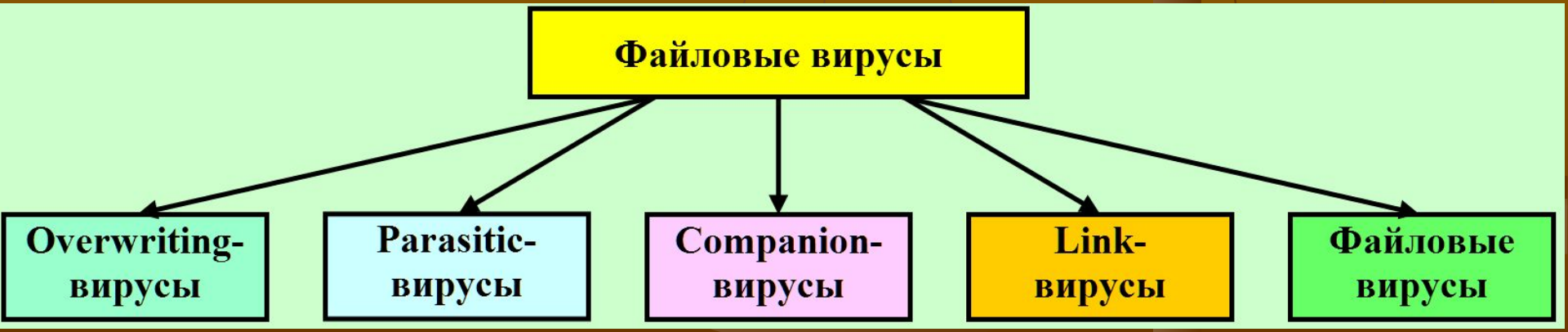
  Таким образом автору вируса, если он желает создать настоящий полиморфик-вирус, не приходится работать над кодами собственного за/расшифровщика. При желании он может подключить к своему вирусу любой известный полиморфик-генератор и вызывать его из кодов вируса. Физически это достигается следующим образом: объектный файл вируса линкуется с объектным файлом генератора, а в исходный текст вируса перед командами его записи в файл вставляется вызов полиморфик-генератора, который создает коды расшифровщика и шифрует тело вируса.

- По **диструктивным** возможностям вирусы можно разделить на:
  - ***безвредные***, т.е. никак не влияющие на работу компьютера (кроме уменьшения свободной памяти на диске в результате своего распространения);
  - ***неопасные***, влияние которых ограничивается уменьшением свободной памяти на диске и графическим, звуковым и прочими эффектами;
  - ***опасные вирусы***, которые могут привести к серьёзным сбоям в работе компьютера;
  - ***очень опасные*** – в алгоритм их работы заведомо заложены процедуры, которые могут вызвать потерю программ, уничтожить данные, стереть необходимую для работы компьютера информацию, записанную в системных областях памяти, и даже, как гласит одна из непроверенных компьютерных легенд, способствовать быстрому износу движущихся частей механизма – вводить в резонанс и разрушать головки некоторых типов винчестеров.

Файловые вирусы

- К данной группе относятся вирусы, которые при своем размножении тем или иным способом используют файловую систему какой-либо (или каких-либо) ОС.
- Файловые вирусы могут внедряться практически во все исполняемые файлы всех популярных ОС. На сегодняшний день известны вирусы, поражающие все типы выполняемых объектов стандартной DOS: командные файлы (BAT), загружаемые драйверы (SYS, в том числе специальные файлы IO.SYS и MSDOS.SYS) и выполняемые двоичные файлы (EXE, COM). Существуют вирусы, поражающие исполняемые файлы других ОС - Windows 3.x, Windows 95/NT, OS/2, Macintosh, Unix, включая VxD-драйверы Windows 3.x и Windows 95.

По способу заражения файлов вирусы делятся на:



- **Overwriting-вирусы**

Данный метод заражения является наиболее простым : вирус записывает свой код вместо кода заражаемого файла, уничтожая его содержимое. Естественно, что при этом файл перестает работать и не восстанавливается. Такие вирусы очень быстро обнаруживают себя, так как ОС и приложения довольно быстро перестают работать. Не известно ни одного случая, когда подобного типа вирусы были бы обнаружены "в живом виде" и стали причиной эпидемии.

- К разновидности overwriting-вирусов относятся вирусы, записывающиеся вместо DOS-заголовка NewEXE-файлов. Основная часть файла при этом остается без изменений и продолжает нормально работать в соответствующе ОС, однако DOS-заголовок оказывается испорченным.

- **Parasitic-вирусы**

К паразитическим относятся все файловые вирусы, которые при распространении своих копий обязательно изменяют содержимое файлов, оставляя сам файлы при этом полностью или частично работоспособными. Основными типами таких вирусов являются вирусы, записывающиеся в начало файлов (*prepending*), в конец файлов (*appending*) и в середину файлов (*inserting*). В свою очередь, внедрение вирусов в середину файлов происходит различнь ми методами - путем переноса части файла в его конец или внедрения в заведомо неиспользуемые данные файла (*cavity-вирусы*).

- **Companion-вирусы**

К категории компаньон-вирусов относятся вирусы, не изменяющие заражаемых файлов. Алгоритм работы этих вирусов состоит в том, что для заражаемого файла создается файл-двойник, причем при запуске зараженного файла управление получает именно этот двойник, т. е. вирус.

- **Link-вирусы**
- Link-вирусы, как и компаньон-вирусы, не изменяют физического содержимого файлов, однако при запуске зараженного файла заставляют ОС выполнить свой код. Этой цели они достигают модификацией необходимых полей файловой системы.
  На сегодняшний день известен единственный тип link-вирусов - вирус семейства ***Dir_II***. При заражении системы они записывают свое тело в последний кластер логического диска. При заражении файла вирусы корректируют лишь номер первого кластера файла, расположенный в соответствующем секторе каталога. Новый начальный кластер файла будет указывать на кластер, содержащий тело вируса. Таким образом, при заражении файлов и длина и содержимое кластеров с этими файлами не изменяются, а на все зараженные файлы на одном логическом диске будет приходиться только одна копия вируса.
- До заражения данные каталога хранят адрес первого кластера файла.
  После заражения данные каталога указывают на вирус, т. е. при запуске файла управление получают не файлы, а вирус.

- **Файловые черви**
- Файловые черви (worms) являются в некотором смысле разновидностью компаньон-вирусов, но при этом никоим образом не связывают свое присутствие с каким-либо выполняемым файлом. При размножении они всего лишь копируют свой код в какие-либо каталоги дисков в надежде, что эти новые копии будут когда-либо запущены пользователем. Иногда эти вирусы дают своим копиям "специальные" имена, чтобы подтолкнуть пользователя на запуск своей копии, например **INSTALL.EXE** или **WINSTART.BAT**.
- Существуют вирусы-черви, использующие довольно необычные приемы, например, записывающие свои копии в архивы (ARJ, ZIP и пр.). К таким вирусам относятся "***ArjVirus***" и "***Winstart***".
- Не следует путать файловые вирусы-черви с сетевыми червями. Первые используют только файловые функции какой-либо операционной системы, вторые же при своем размножении пользуются сетевыми протоколами.

Алгоритм работы файлового вируса

Получив управление, вирус совершает следующие действия:

(приводится список наиболее общих действий вируса при его выполнении; для конкретного вируса список может быть дополнен, пункты могут поменяться местами и значительно расшириться):

- резидентный вирус проверяет оперативную память на наличие своей копии и инфицирует память компьютера, если копия вируса не найдена; резидентный вирус ищет незараженные файлы в текущем и (или) корневом каталогах, в каталогах, отмеченных командой PATH, сканирует дерево каталогов логических дисков, а затем заражает обнаруженные файлы;
- выполняет, если они есть, дополнительные функции: деструктивные действия, графические или звуковые эффекты и т. д. (дополнительные функции резидентного вируса могут вызываться спустя некоторое время после активизации в зависимости от текущего времени, конфигурации системы, внутренних счетчиков вируса или других условий; в этом случае вирус при активизации обрабатывает состояние системных часов, устанавливает свои счетчики и т. д.);
- возвращает управление основной программе (если она есть). Паразитические вирусы при этом либо восстанавливают программу (но не файл) в исходном виде (например, у COM-программы восстанавливается несколько первых байтов, у EXE-программы вычисляется истинный стартовый адрес, драйвера восстанавливаются значения адресов программ стратегии и прерывания), либо лечат файл, выполняют его, а затем снова заражают. Компаньон-вирусы запускают на выполнение своего "хозяина", вирусы-черви и overwriting-вирусы возвращают управление DOS.

Загрузочные вирусы

- Загрузочные вирусы заражают загрузочный (**boot**) сектор гибкого диска в **boot-сектор** или **Master Boot Record** (MBR) винчестера. Принцип действия загрузочных вирусов основан на алгоритмах запуска ОС при включении или перезагрузке компьютера: после необходимых тестов установленного оборудования (памяти, дисков и т. д.) программа системной загрузки считывает первый физический сектор загрузочного диска и передает управление на A:, C: или CD-ROM, в зависимости от параметров, установленных BIOS Setup.
- При заражении дисков загрузочные вирусы подставляют свой код вместо какой-либо программы, получающей управление при загрузке системы. Принцип заражения, таким образом, одинаков во всех описанных выше способах: вирус "заставляет" систему при ее перезапуске считать в память и отдать управление не оригинальному коду загрузчика, а коду вируса.
- Заражение дискет производится единственным известным способом: вирус записывает свой код вместо оригинального кода boot-сектора дискеты. Винчестер заражается тремя возможными способами: вирус записывается либо вместо кода MBR, либо вместо кода boot-сектора загрузочного диска (обычно диска C:), либо модифицирует адрес активного boot-сектора в Disk Partition Table, расположенный в MBR винчестера.

Алгоритм работы загрузочного вируса

Практически все загрузочные вирусы резидентны. Они внедряются в память компьютера при загрузке с инфицированного диска. При этом системный загрузчик считывает содержимое первого сектора диска, с которого производится загрузка, помещает считанную информацию в память и передает на нее (т. е. на вирус) управление. После этого начинают выполняться инструкции вируса, который:

- как правило, уменьшает объем свободной памяти (слово по адресу 0040:0013), копирует в освободившееся место свой код и считывает с диска свое продолжение (если оно есть). В дальнейшем некоторые вирусы ждут загрузки DOS и восстанавливают это слово в его первоначальном значении. В результате они оказываются расположенными не за пределами DOS, а как отдельные блоки DOS-памяти;
- перехватывает необходимые векторы прерываний (обычно - INT 13H), считывает в память оригинальный boot-сектор и передает на него управление.
- В дальнейшем загрузочный вирус ведет себя так же, как резидентный файловый: перехватывает обращения ОС к дискам и инфицирует их, в зависимости от некоторых условий совершает деструктивные действия или вызывает звуковые или видеоэффекты.

Макровирусы

Макровирусы (*macro viruses*) являются программами на языках (макроязыках), встроенных в некоторые системы обработки данных (текстовые редакторы, электронные таблицы и т. д.). Для своего размножения такие вирусы используют возможности макроязыков и при их помощи переносят себя из одного зараженного файла (документа или таблицы) в другие.

Наибольшее распространение получили макровирусы для ***Microsoft Word, Excel и Office 97.***

Для существования вирусов в конкретной системе необходимо наличие встроенного в систему макроязыка с возможностями:

1) привязки программы на макроязыке к конкретному файлу;
2) копирования макропрограмм из одного файла в другой;
3) получения управления макропрограммой без вмешательства пользователя (автоматические или стандартные макросы).

Данным условиям удовлетворяют редакторы ***Microsoft Word***, ***Office 97*** и ***AmiPro***, а также электронная таблица ***Excel***. Эти системы содержат себе макроязыки (**Word - Word Basic, Excel и Office 97 - Visual Basic**), а также:

1) макропрограммы привязаны к конкретному файлу (AmiPro) или находятся внутри файла (Word, Excel, Office 97);
2) макроязык позволяет копировать файлы (AmiPro) или перемещать как подпрограммы в служебные файлы системы и редактируемые файлы (Word, Excel, Office 97);
3) при работе с файлом при определенных условиях (открытие, закрытие и т. д.) вызываются макропрограммы (если таковые есть), которые определены специальным образом (AmiPro) или имеют стандартные имена (Word, Excel, Office 97).

- Эта особенность макроязыков предназначена для автоматической обработки данных в больших организациях или в глобальных сетях и позволяет организовать так называемый "автоматизированный документооборот". С другой стороны, возможности макроязыков таких систем позволяют вирусу переносить свой код в другие файлы и заражать их.
- На сегодняшний день известны четыре системы, для которых существуют вирусы, - Microsoft Word, Excel, Office 97 и AmiPro. В этих системах вирус получают управление при открытии или закрытии зараженного файла, перехватывают стандартные файловые функции и затем заражают файлы, к которым каким-либо образом идет обращение. По аналогии с MS-DOS можно сказать, что большинство макровирусов являются резидентными: они активны не только в момент открытия/закрытия файла, но до тех пор, пока активен сам редактор.

Макровирусы, поражающие файлы Word, Excel или Office 97, как правило, пользуются одним из трех приемов: в вирусе либо присутствует автомакрос (автофункция), либо переопределен один из стандартных системных макросов (ассоциированный с каким-либо пунктом меню), либо макрос вируса вызывается автоматически при нажатии на какую-либо клавишу или комбинацию клавиш. Существуют также полувирусы, которые не используют всех этих приемов и размножаются, только когда пользователь самостоятельно запускает их на выполнение.

- Таким образом, если документ заражен, при его открытии Word вызывает зараженный автоматический макрос AutoOpen (или AutoClose при закрытии документа) и запускает код вируса, если это не запрещено системной переменной DisableAutoMacros. Если вирус содержит макросы со стандартными именами, они получают управление при вызове соответствующего пункта меню (File/Open, File/Close, File/SaveAs). Если же переопределен какой-либо символ клавиатуры, то вирус активизируется только после нажатия на соответствующую клавишу.

- **Сетевые вирусы**
- К сетевым относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. "Полноценные" сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свои код на удаленном компьютере или, по крайней мере, "подтолкнуть" пользователя к запуску зараженного файла.
- Бытует ошибочное мнение, что сетевым является любой вирус, распространяющийся в компьютерной сети. Но в таком случае практически все вирусы были бы сетевыми, даже наиболее примитивные из них: ведь самый обычный нерезидентный вирус при заражении файлов не разбирается, сетевой (удаленный) это диск или локальный. В результате такой вирус способен заражать файлы в пределах сети, но отнести его к сетевым никак нельзя.

Наибольшую известность приобрели сетевые вирусы конца 80-х, их так же называют ***сетевыми червями*** (worms). К ним относятся вирус ***Морриса***, вирусы ***Cristmas Tree*** и ***Wank Worm***. Для своего распространения они использовали ошибки и недокументированные функции глобальных сетей того времени. Вирусы передавали свои копии с сервера на сервер и запускали их на выполнение. Эпидемия вируса Морриса захватила в свое время несколько глобальных сетей в США.

Прочие вредные программы

К вредным программам помимо вирусов относятся также "***троянские кони***" (логические бомбы), ***intended-вирусы***, ***конструкторы вирусов*** и ***полиморфик-генераторы***.

"Троянский конь" - это программа, наносящая какие-либо разрушительные действия, т. е. в зависимости от определенных условий или при каждом запуске уничтожающая информацию на дисках, "приводящая" систему (к зависанию) и т. п.

Большинство известных "троянских коней" подделываются под какие-либо полезные программы, новые версии популярных утилит или дополнения к ним. Очень часто они рассылаются по BBS-станциям или электронным конференциям. По сравнению с вирусами "троянские кони" не получают широкого распространения по достаточно простым причинам: они либо уничтожают себя вместе с остальными данными на диске, либо демаскируют свое присутствие и уничтожаются пострадавшим пользователем.

- Следует отметить также "***злые шутки***" (hoax). К ним относятся программы, которые не причиняют компьютеру какого-либо прямого вреда, однако выводят сообщения о том, что такой вред уже причинен, либо будет причинен при каких-либо условиях, либо предупреждают пользователя о несуществующей опасности. К "злым шуткам" относятся, например, программы, которые "пугают" пользователя сообщениями о форматировании диска (хотя никакого форматирования на самом деле не происходит), определяют вирусы в незараженных файлах (как это делает широко известная программа ***ANTITIME***), выводят странные вирусоподобные сообщения (драйвер диска CMD640X от какого-то коммерческого пакета) и т. д. - варианты зависят от чувства юмора автора такой программы. Видимо, к "злым шуткам" относится также строка ***CHOLEEPA*** во втором секторе винчестеров фирмы Seagate. К этой же категории шуток можно отнести заведомо ложные сообщения о новых супервирусах. Такие сообщения периодически появляются в электронных конференциях и обычно вызывают среди пользователей панику.

"Стелс"-вирусы

"Стелс"-вирусы теми или иными способами скрывают факт своего присутствия в системе. Известны "стелс"-вирусы всех типов за исключением Windows-вирусов, файловые DOS-вирусы и даже макровирусы. Появление "стелс"-вирусов, заражающих файлы Windows, скорее всего дело времени.

Загрузочные "стелс"-вирусы для скрытия своего кода используют два основных способа.

Первый из них заключается в том, что вирус перехватывает команды чтения зараженного сектора (INT 13h) и подставляет вместо него незараженный оригинал. Этот способ делает вирус невидимым для любой DOS-программы, включая антивирусы, неспособные "лечить" оперативную память компьютера. Возможен перехват команд чтения секторов на уровне более низком, чем INT 13h.

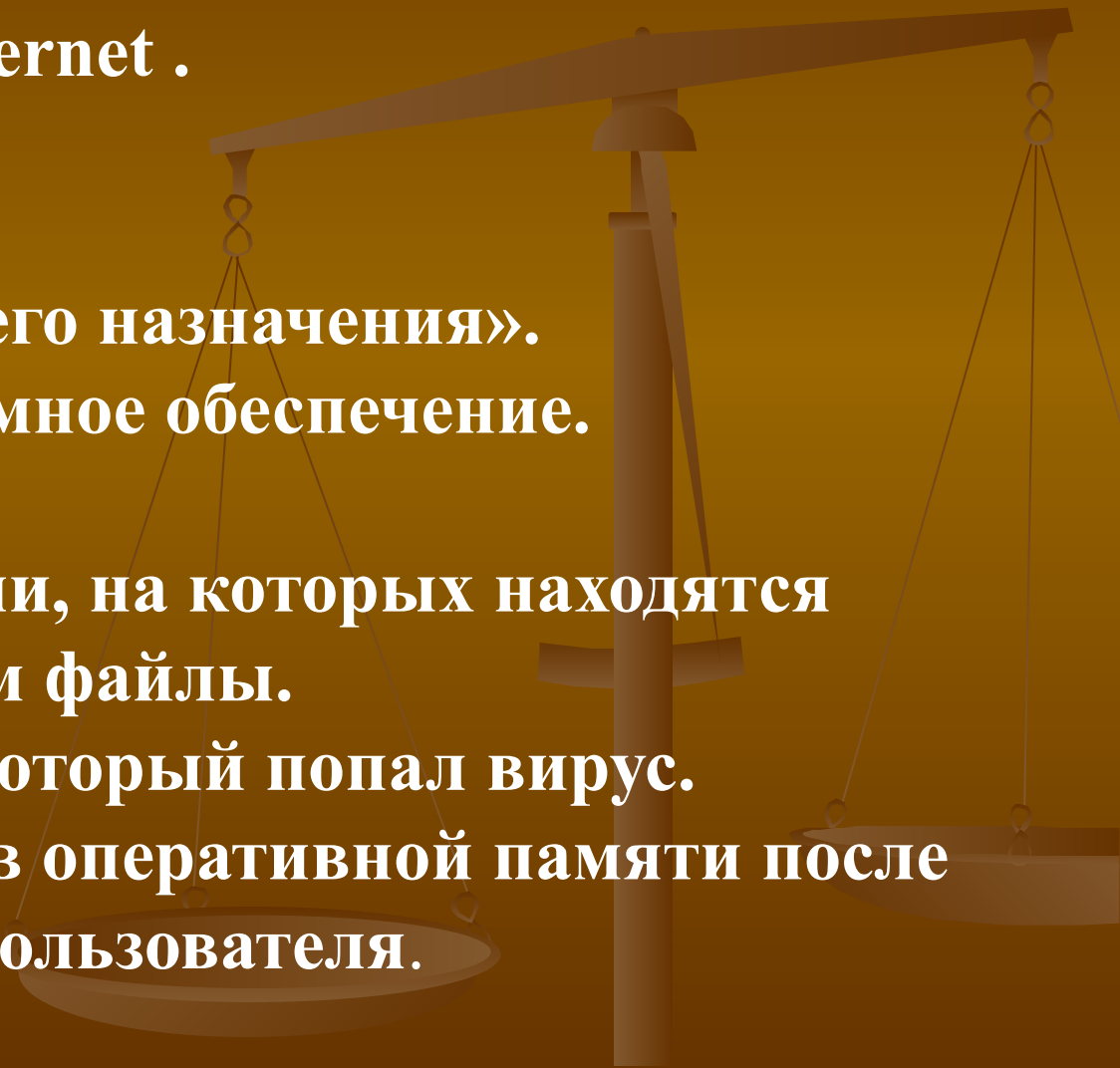
Второй способ направлен против антивирусов, поддерживающих команды прямого чтения секторов через порты контроллера диска. Такие вирусы при запуске любой программы (включая антивирус) восстанавливают зараженные сектора, а после окончания ее работы снова заражают диск. Поскольку для этого вирусу приходится перехватывать запуск и окончание работы программ, то он должен перехватывать также DOS-прерывание INT 21h.

Большинство файловых "стелс"-вирусов использует те же приемы, что приведены выше: они либо перехватывают DOS-вызовы обращения к файлам (INT21h), либо временно лечат файл при его открытии и заражают при закрытии. Так же как и для загрузочных вирусов, существуют файловые вирусы, использующие для своих "стелс"-функций перехват прерываний более низкого уровня - вызовы драйверов DOS, INT 25h и даже INT 13h. Полноценные файловые "стелс"-вирусы, использующие первый способ скрытия своего кода, в большинстве своем достаточно громоздки, поскольку им приходится перехватывать большое количество DOS-функций работы с файлами: открытие-закрытие, чтение-запись, поиск, запуск, переименование и т.д., причем необходимо поддерживать оба варианта некоторых вызовов (FCB/ASCII), а с появлением Windows 95/NT необходимо также обрабатывать третий вариант - функции работы с длинными именами файлов.

- **Полиморфик-вирусы**
- Полиморфик-вирусами являются те, обнаружение которых невозможно , или крайне затруднительно осуществить при помощи так называемых вирусных масок - участков постоянного кода, специфичных для конкретного вируса. Достигается это двумя основными способами - шифрованием основного кода вируса с непостоянным ключом и случайным набором команд расшифровщика или изменением самого выполняемого кода вируса. Существуют также другие, достаточно экзотические примеры полиморфизма - DOS-вирус Bomber, например, не зашифрован, однако последовательность команд, которая передает управление коду вируса, является полностью полиморфной.
  Полиморфизм различной степени сложности встречается в вирусах всех типов - от загрузочных и файловых DOS-вирусов до Windows-вирусов и даже макровирусов.

Пути проникновения вирусов на компьютер:

- Глобальная сеть Internet .
- Электронная почта.
- Локальная сеть.
- Компьютеры «Общего назначения».
- Пиратское программное обеспечение.
- Ремонтные службы.
- Съемные накопители, на которых находятся заражённые вирусом файлы.
- Жёсткий диск, на который попал вирус.
- Вирус, оставшийся в оперативной памяти после предшествующего пользователя.



3. Методы защиты от компьютерных вирусов

1. Установите на свой персональный компьютер современную антивирусную программу.
2. Перед просмотром информации принесенной на флэш-карте (дискете) с другого компьютера проверьте носитель антивирусом.
3. После разархивирования архивных файлов сразу проверьте их на вирусы (не все антивирусные программы могут искать вредоносный код в архивах или могут делать это не корректно).
4. Периодически проверяйте компьютер на вирусы (если активно пользуетесь Интернетом – запускайте раз в неделю, а то и чаще).
5. Как можно чаще делайте резервные копии важной информации (backup).
6. Используйте совместно с антивирусной программой файервол (firewall) если компьютер подключен к Интернет.
7. Настройте браузер (программа просмотра Интернет страниц – IE, Opera и т.д.) для запрета запуска активного содержимого html-страниц.

- **Файрвол** (англ. *firewall*, от *fire* «огонь» + *wall* «стена») означает:
- Межсетевой экран (брандмауэр) — технологический барьер, предназначенный для предотвращения несанкционированного или нежелательного сообщения между компьютерными сетями или хостами:
  - Персональный файрвол — популярная форма файрвола, предназначенная для защиты персональных компьютеров.
- **Файерволы** анализируют поток данных (трафик) в сети. Блокируют проникновение вредоносных программ из внешней сети.
- **Антивирусные программы** отслеживают проявление вредоносных программ непосредственно на компьютере пользователя.

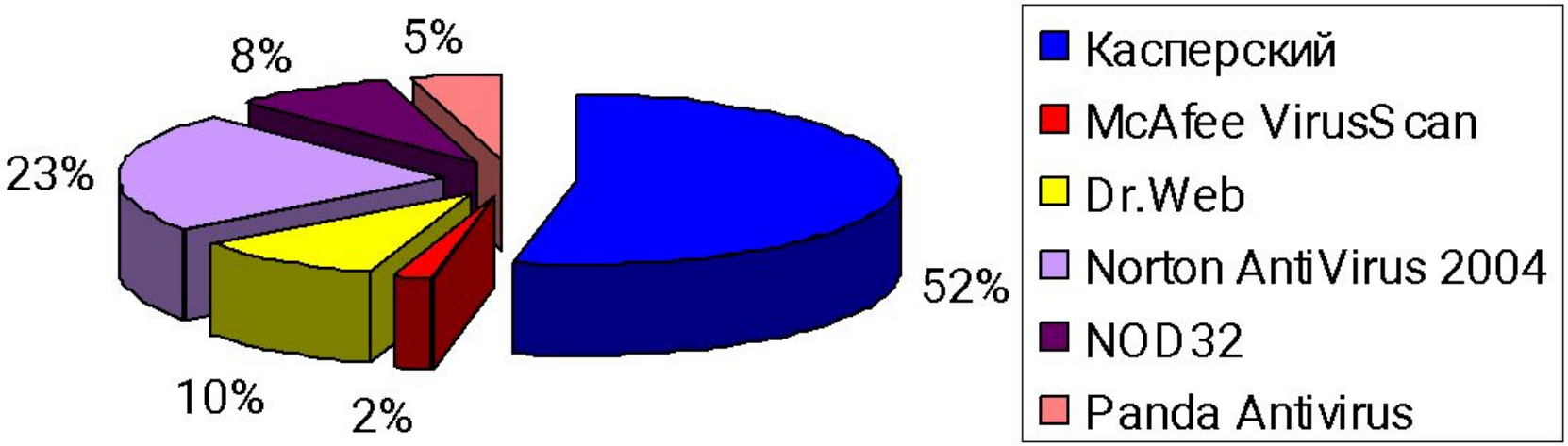
На современном этапе развития антивирусной защиты многие производители данного программного обеспечения стараются сделать так, чтобы их программный продукт включал в себя как функции фаервола, так и антивируса. Это позволяет пользователю максимально защитить свой компьютер и от несанкционированного проникновения, и от вредоносных программ.

Антивирусные программы

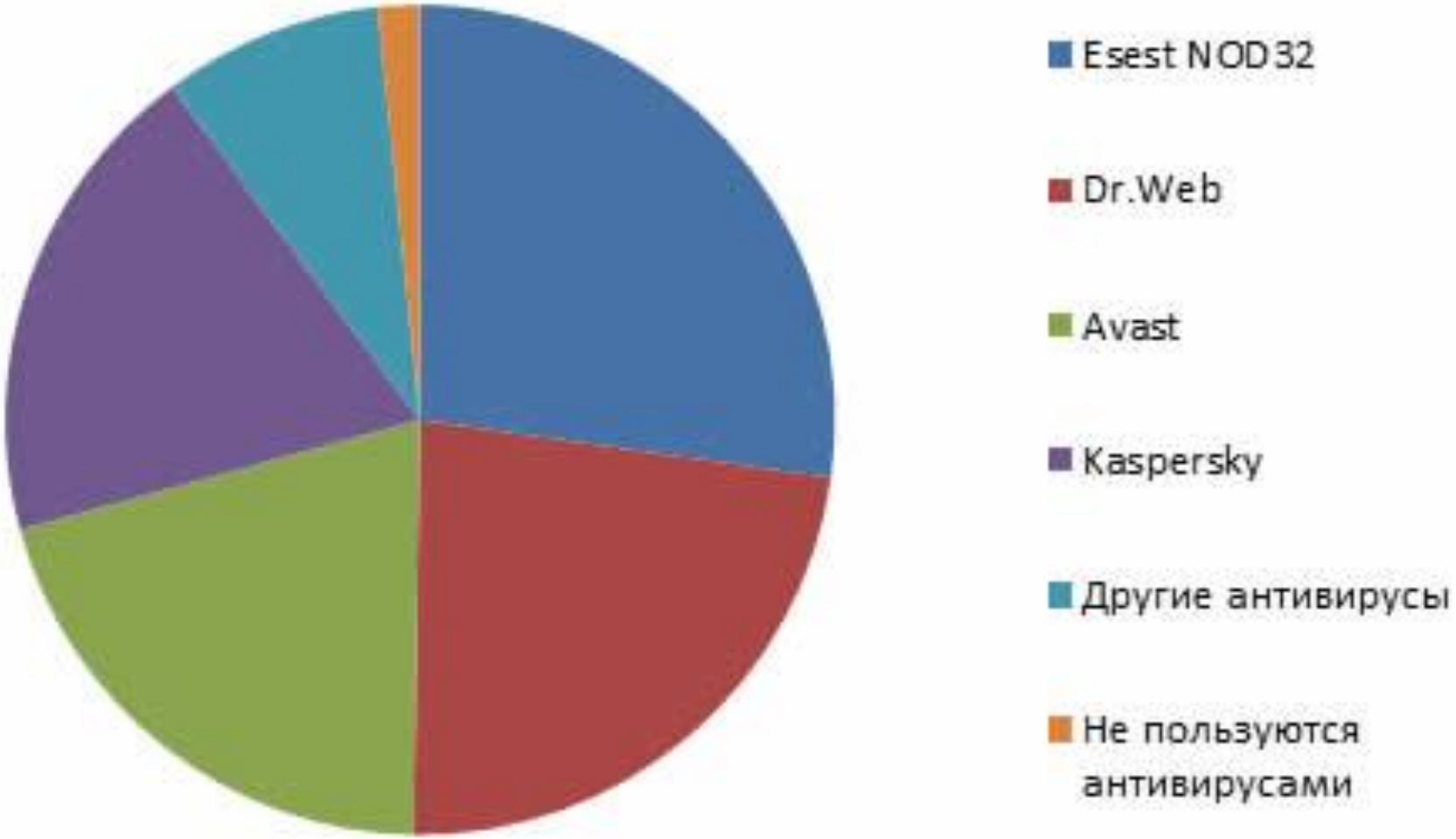
предназначены для предотвращения заражения компьютера вирусом и ликвидации последствий заражения.

Опрос пользователей ПК.

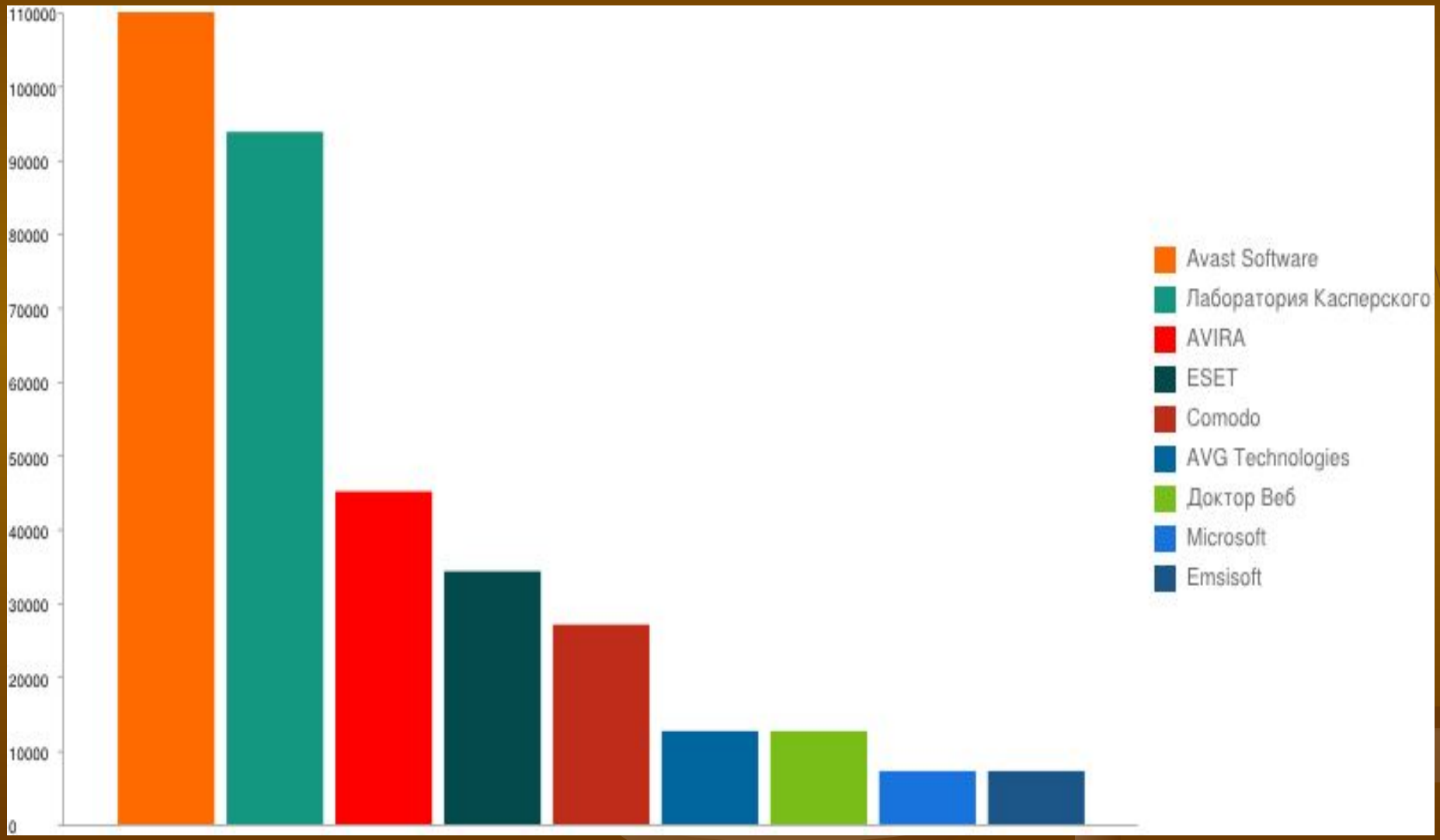
Популярность антивирусных программ.



Рейтинг лучших антивирусов 2010 г.

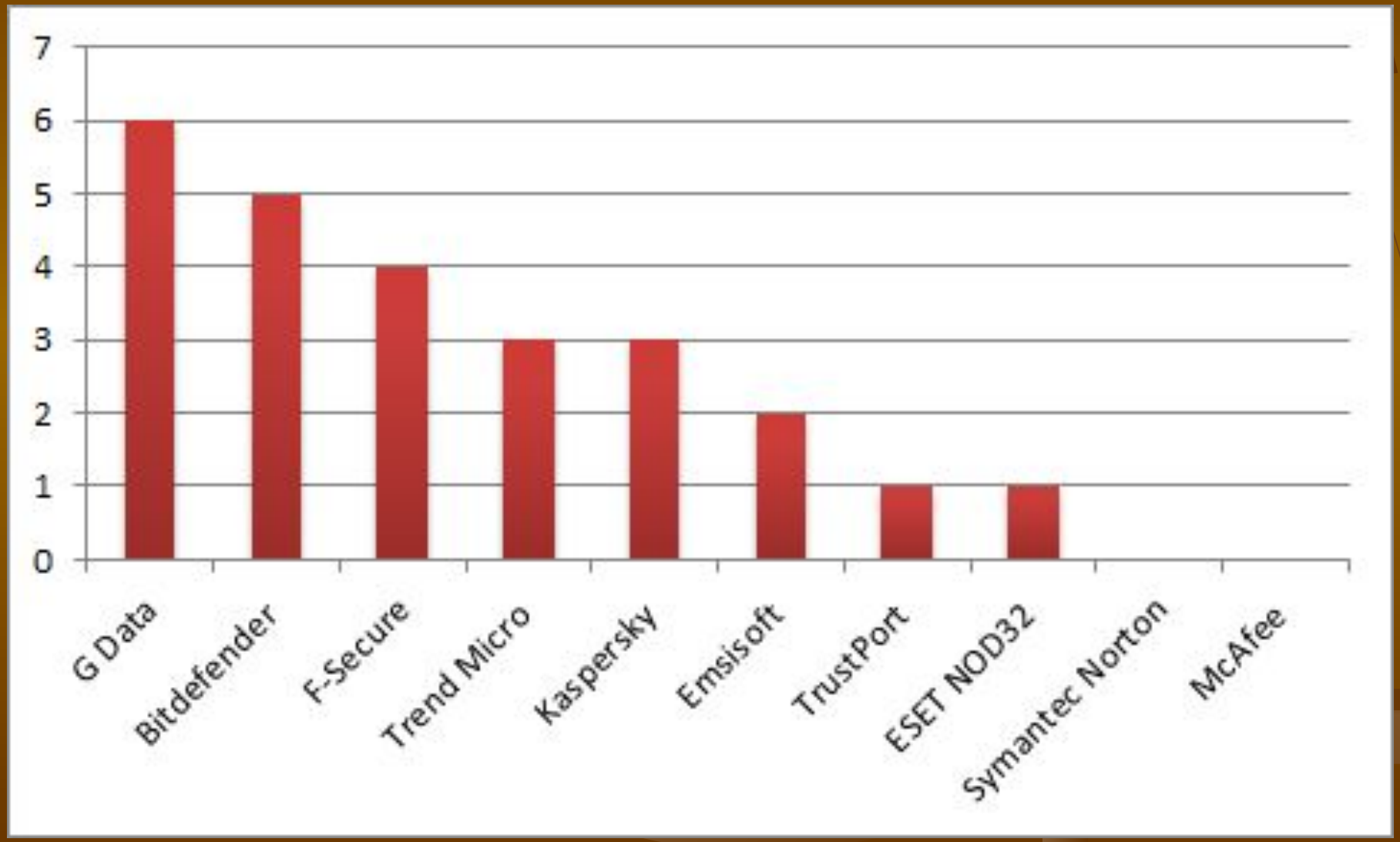


Статистика вендоров (фирм-производителей)



Рейтинги антивирусных программ.

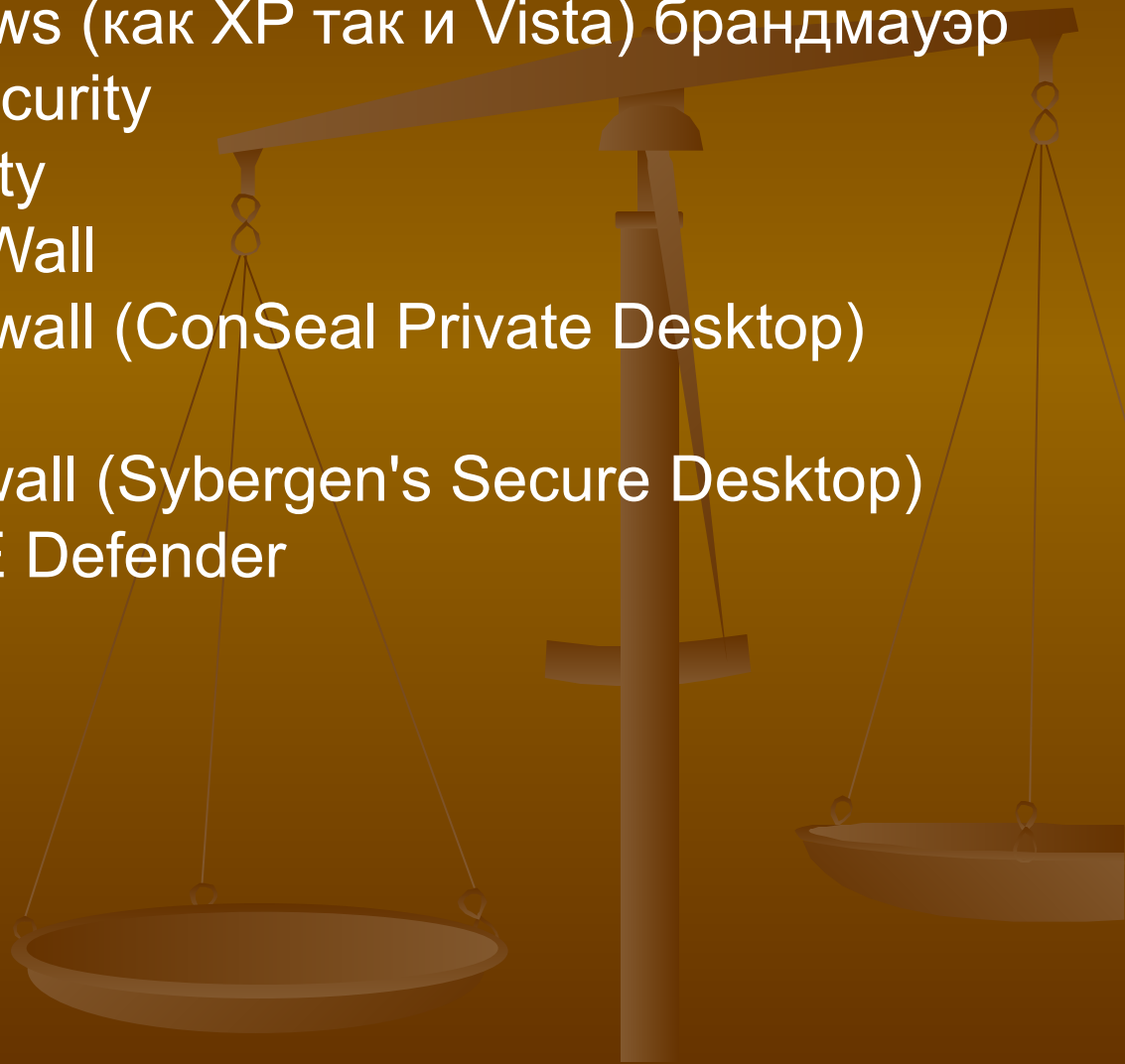
Количество максимальных наград по уровню защиты, полученных в указанных тестированиях:



Наиболее популярные фаерволы

1. Встроенный в Windows (как XP так и Vista) брандмауэр
2. Kaspersky Internet Security
3. Norton Internet Security
4. Agnitum Outpost FireWall
5. McAfee Personal Firewall (ConSeal Private Desktop)
6. Look'n'Stop
7. Sygate Personal Firewall (Sybergen's Secure Desktop)
8. Network Ice Black ICE Defender
9. Zone Alarm

и др.



Три вирусные аксиомы

Во-первых, **вирусы не возникают сами собой** - их создают нехорошие программисты-хакеры и рассылают по сети передачи данных или подкидывают на компьютеры знакомых.

Во-вторых: **вирус не может сам собой появиться на Вашем компьютере** - либо его подсунули на дискетах или даже на компакт-диске, либо Вы его случайно скачали из компьютерной сети, либо вирус жил у Вас в компьютере с самого начала, либо (что самое ужасное) программист-хакер живет у Вас в доме.

В третьих: **компьютерные вирусы заражают только компьютер** и ничего больше, поэтому не надо бояться - через клавиатуру и мышь они не передаются.

Антивирусные программы

DrWeb

ADinf32

Avast

Norton Antivirus

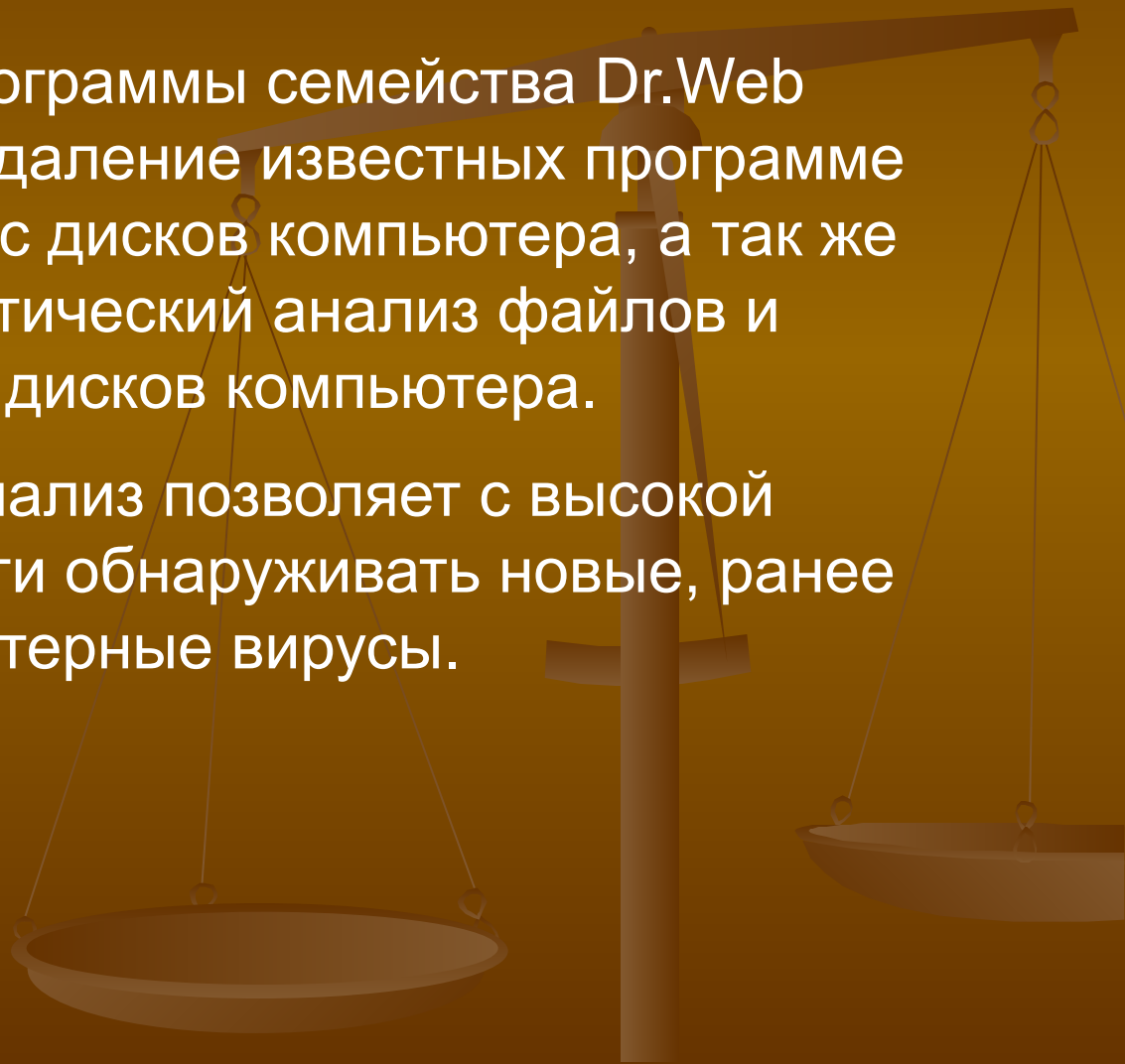
Антивирус Касперского

Антивирус NOD32

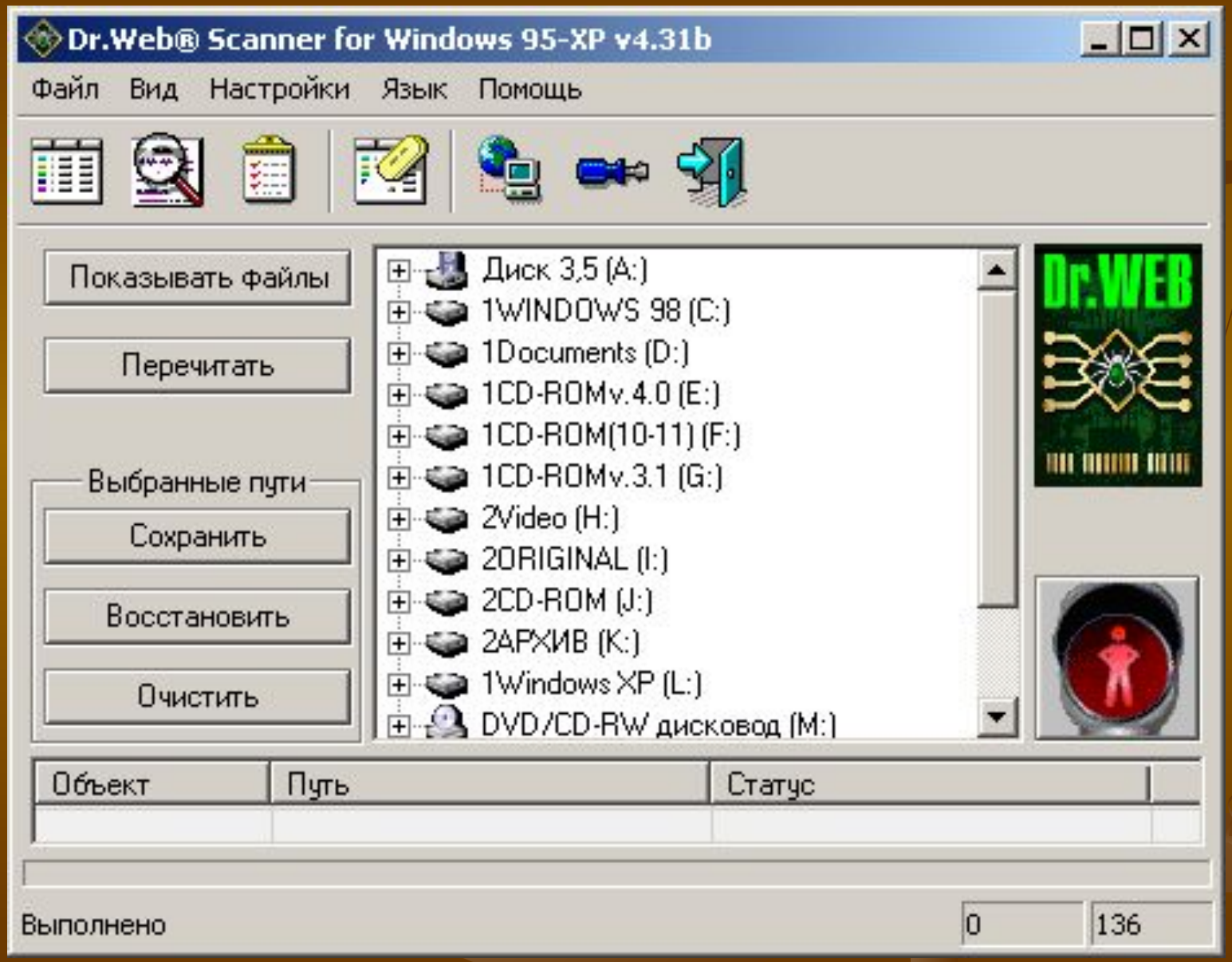
DrWeb

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.



DrWeb


Dr.Web® Scanner for Windows 95-XP v4.31b
Файл
Вид
Настройки
Язык
Помощь
Показывать файлы
Перечитать
Выбранные пути
Сохранить
Восстановить
Очистить
Диск 3,5 (A:)
1WINDOWS 98 (C:)
1Documents (D:)
1CD-ROMv.4.0 (E:)
1CD-ROM(10-11) (F:)
1CD-ROMv.3.1 (G:)
2Video (H:)
2ORIGINAL (I:)
2CD-ROM (J:)
2АРХИВ (K:)
1Windows XP (L:)
DVD/CD-RW дисковод (M:)
Dr.WEB
Объект
Путь
Статус
Выполнено
0
136

ADinf32

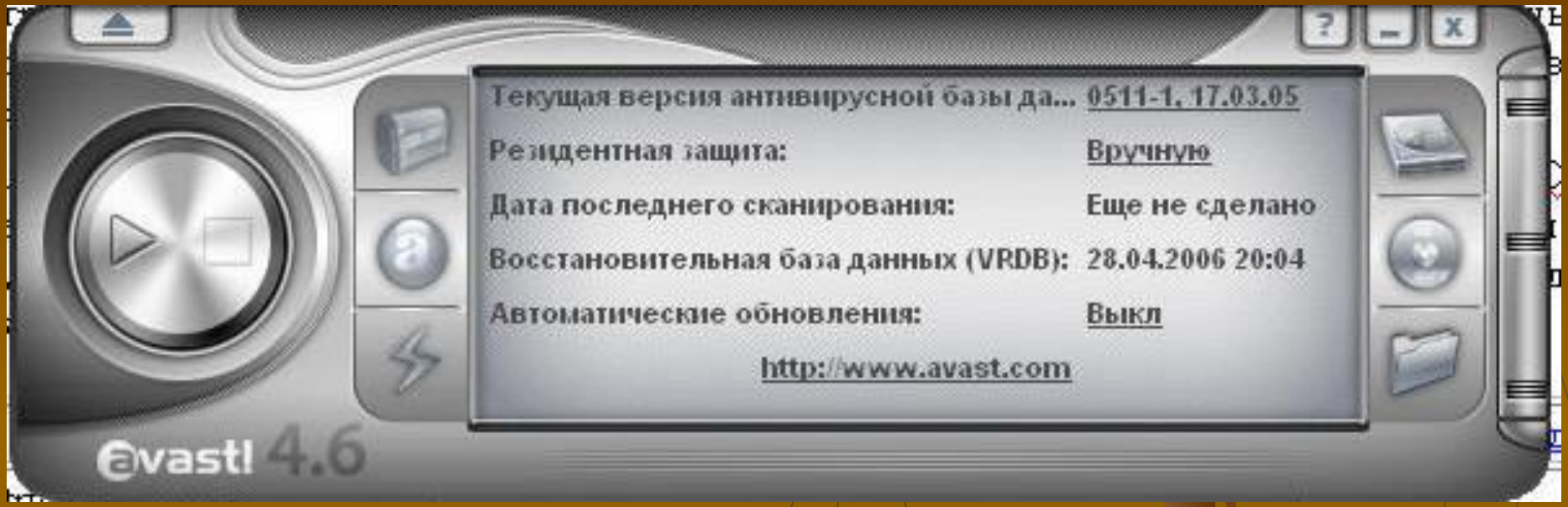
Ревизор диска ADinf32 - современное средство для защиты от вирусов и для контроля целостности и сохранности информации на вашем диске. Эта антивирусная программа фиксирует любые изменения в файловой системе компьютера и обладает удобным пользовательским интерфейсом. Программа ADinf на протяжении многих лет заслуженно являются самыми популярными в России ревизорами файловых систем и успешно используются.

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

ADinf32

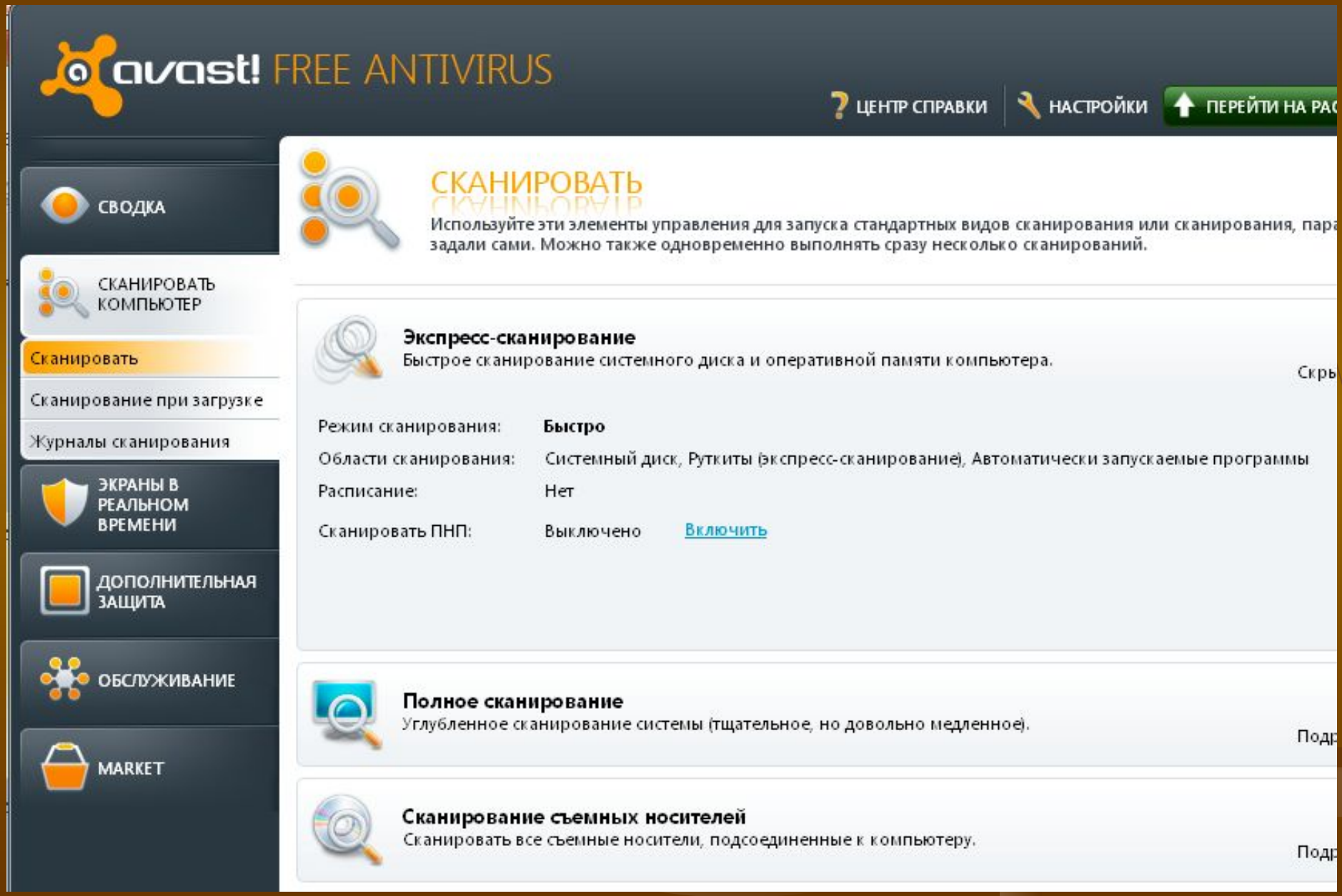

ADinf32 v3.00/30-дневная ознаком. версия (Настройки по умолча...
Advanced Diskinfoscope™
http://www.adinf.com
Рабочий стол
Мой компьютер
Дискета 3,5" A:
Диск C: 12 дек 2000 г.
Диск D: 12 дек 2000 г.
Диск E: 12 дек 2000 г.
Режимы
Без CRC
Не обнов.
Настройки
Старт
Выход
Диски:
Готово 0 из 0
Нажмите "Старт" для начала работы или F1 для помощи

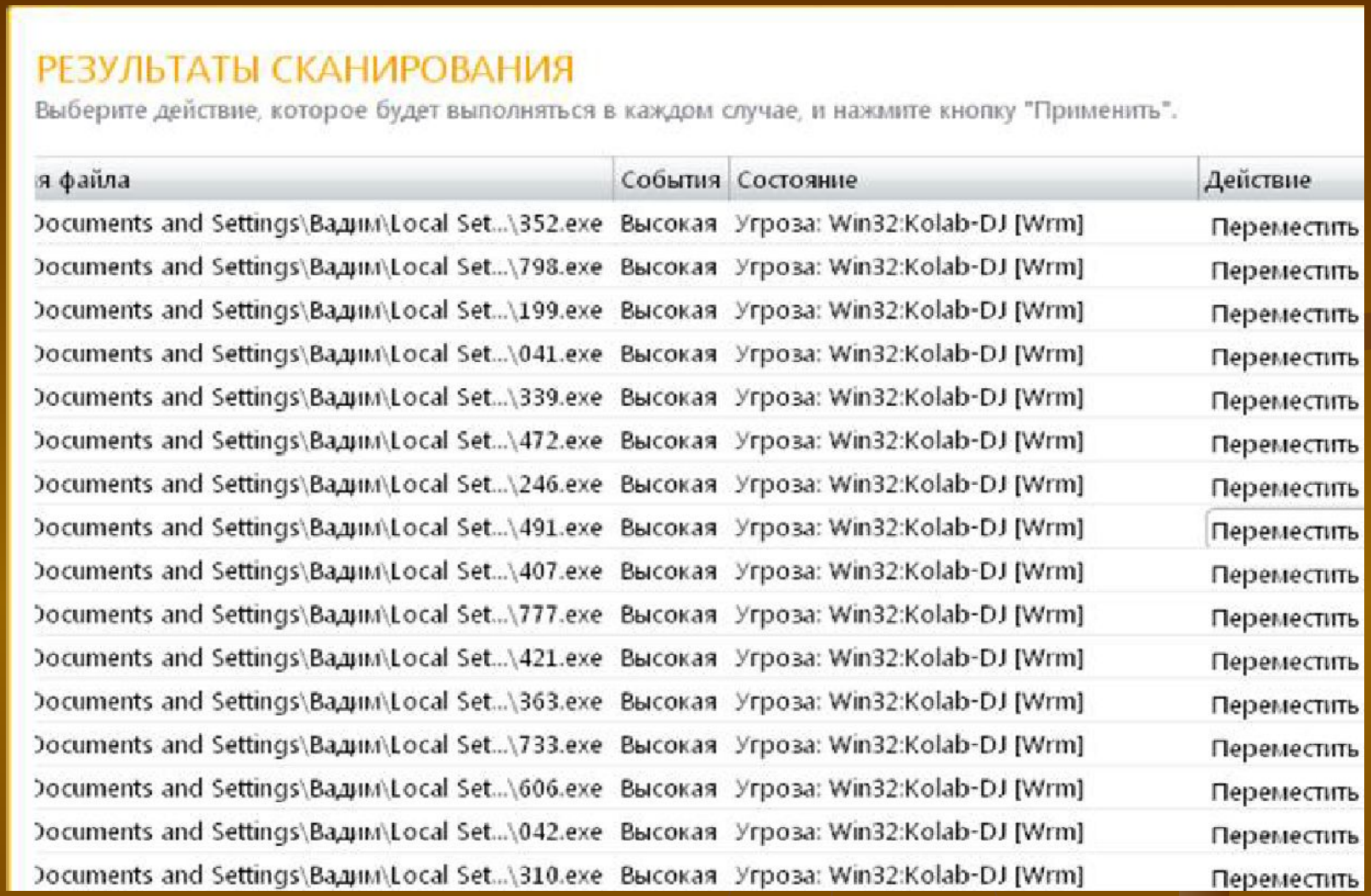
Avast



Avast! - это пакет приложений, предназначенных для защиты компьютера от возможного заражения вирусами и от других угроз со стороны вредоносных программ. При правильном использовании avast! в сочетании с такими программами, как утилиты для резервного копирования данных, существенно снижает риск того, что ваш компьютер подвергнется воздействию вирусов или будет заражен ими - а значит, и уменьшает опасность утраты важных деловых или личных данных.

Avast

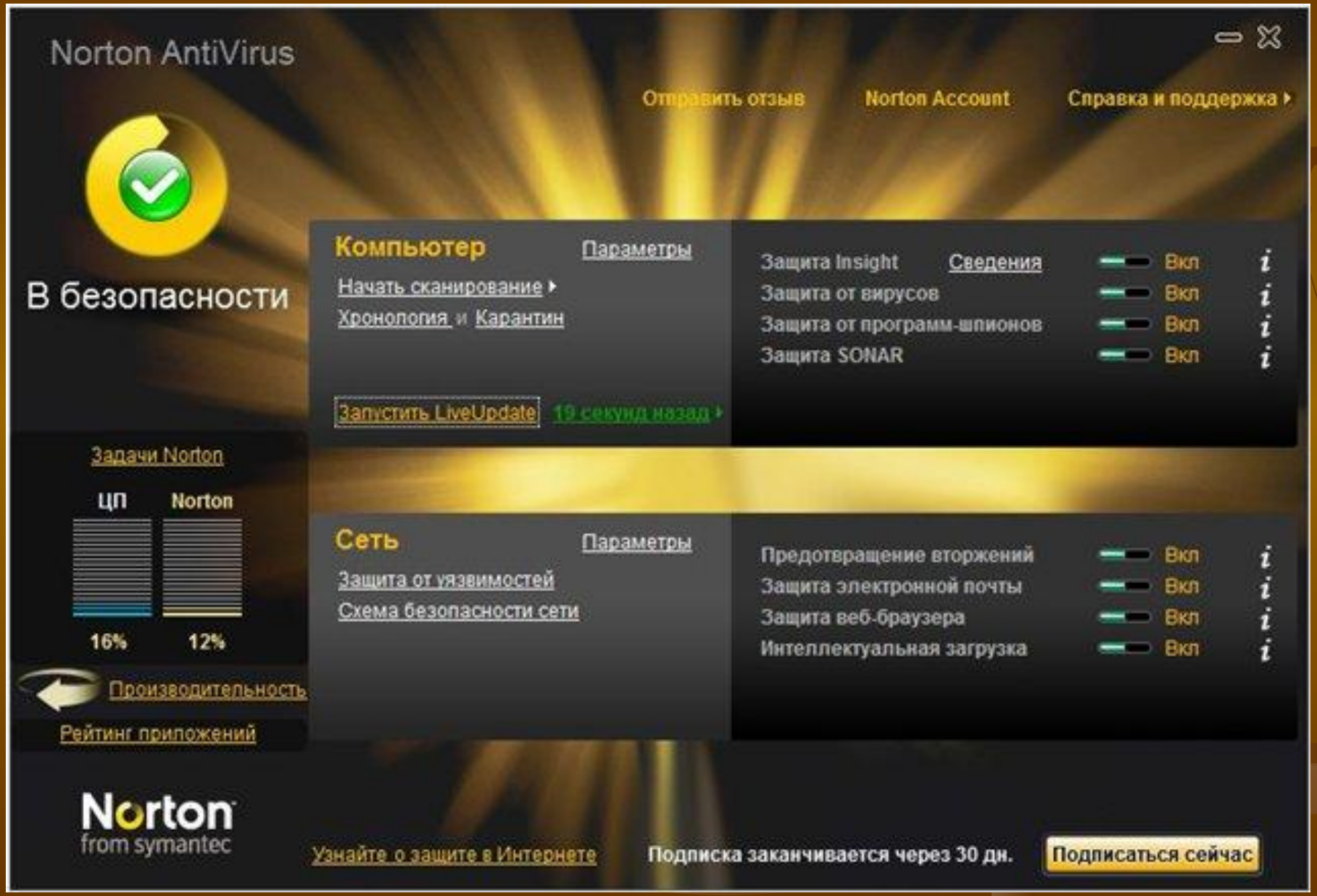

avast! FREE ANTIVIRUS
ЦЕНТР СПРАВКИ
НАСТРОЙКИ
ПЕРЕЙТИ НА РАС
СВОДКА
СКАНИРОВАТЬ КОМПЬЮТЕР
Сканировать
Сканирование при загрузке
Журналы сканирования
ЭКРАНЫ В РЕАЛЬНОМ ВРЕМЕНИ
ДОПОЛНИТЕЛЬНАЯ ЗАЩИТА
ОБСЛУЖИВАНИЕ
MARKET
СКАНИРОВАТЬ
Используйте эти элементы управления для запуска стандартных видов сканирования или сканирования, пара
задали сами. Можно также одновременно выполнять сразу несколько сканирований.
Экспресс-сканирование
Быстрое сканирование системного диска и оперативной памяти компьютера.
Скры
Режим сканирования: Быстро
Области сканирования: Системный диск, Руткиты (экспресс-сканирование), Автоматически запускаемые программы
Расписание: Нет
Сканировать ПНП: Выключено Включить
Полное сканирование
Углубленное сканирование системы (тщательное, но довольно медленное).
Подр
Сканирование съемных носителей
Сканировать все съемные носители, подсоединенные к компьютеру.
Подр



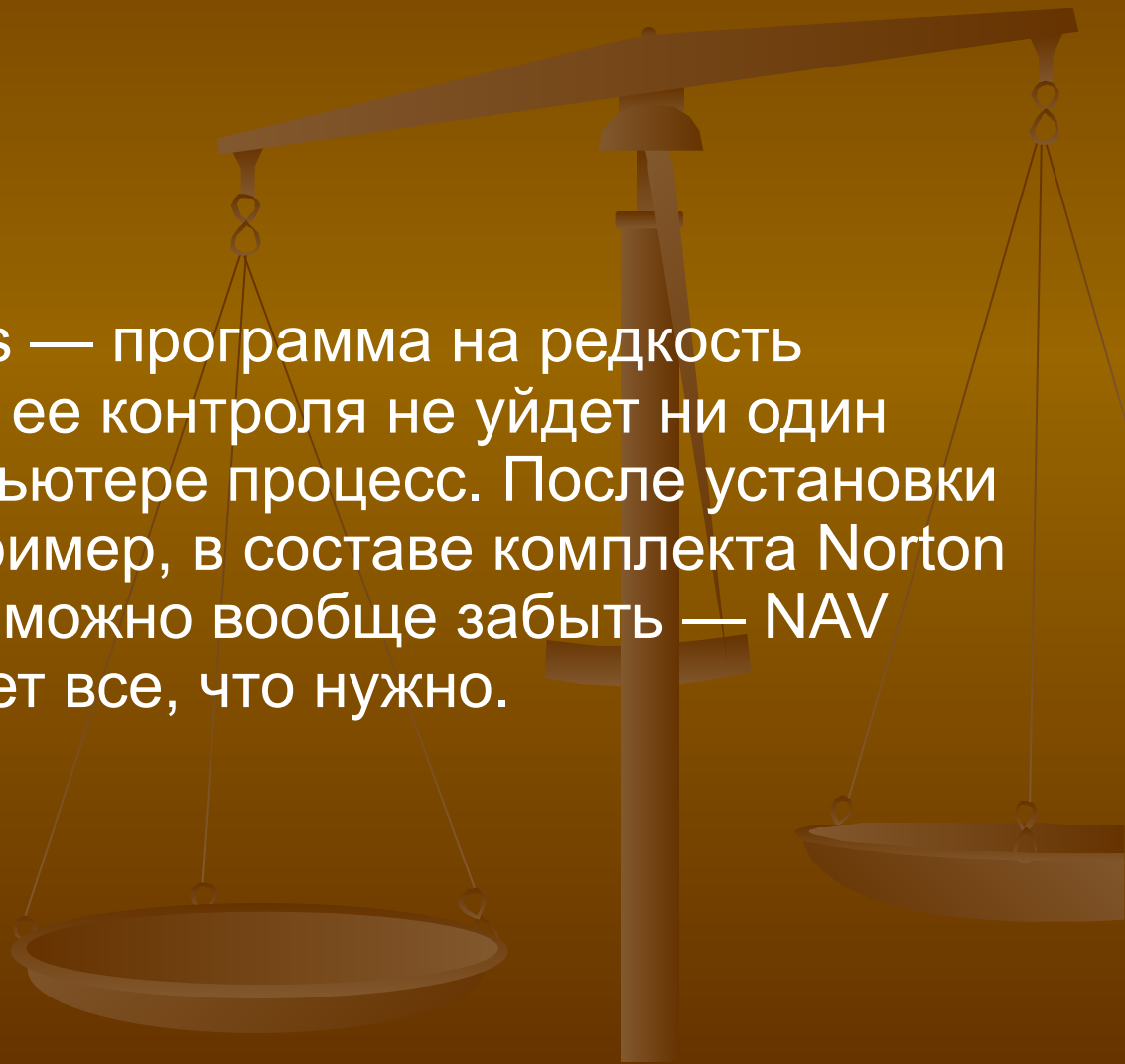
Антивирус avast включает технологию для защиты от "шпионских программ", модуль защиты от руткитов и надежный модуль самозащиты.

К достоинствам **Avast** является наличие бесплатной версии. Хотя в этом случае вы получите не все возможности программы.

Norton Antivirus



Norton Antivirus является «самым-самым» сразу по целому ряду позиций. Самый красивый, самый логично устроенный. Обладатель самой большой базы данных вирусов.



Norton Antiviras — программа на редкость «въедливая», из-под ее контроля не уйдет ни один запущенный на компьютере процесс. После установки Norton Antivirus (например, в составе комплекта Norton System Works) о ней можно вообще забыть — NAV сама проконтролирует все, что нужно.

Антивирус Касперского

Антивирус Касперского 2012 это:
- Базовая защита компьютера
- Передовые антивирусные технологии
- Защита в режиме реального времени
- Базовая защита при работе в интернете и с электронной почтой
- Минимальное влияние на работу компьютера
- Новый интуитивно понятный интерфейс

Антивирус Касперского

В состав Kaspersky AntiVirus Personal Pro входят:

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

AVP Сканер проверяет на наличие вирусов оперативную память, файлы, включая архивные и упакованные, системные сектора, содержащие Master Boot Record, загрузочный сектор (Boot-сектор) и таблицу разбиения диска (Partition Table).

AVP Монитор – резидентный модуль, находящийся постоянно в оперативной памяти компьютера и отслеживающий все файловые операции в системе. Позволяет обнаружить и удалить вирус до момента реального заражения системы в целом.

AVP Центр управления обеспечивает удобный пользовательский интерфейс, создание, сохранение и загрузку большого количества различных настроек, механизм проверки целостности антивирусной системы, мощную систему помощи.

Антивирус Касперского® 2012 – это решение для базовой защиты компьютера от вредоносных программ.

Продукт содержит основные инструменты для обеспечения безопасности ПК. Для полноценной защиты компьютера рекомендуется дополнительно использовать сетевой экран.

Реализует проверку файлов, веб-страниц, почтовых и ICQ-сообщений .

Обеспечивает блокирование ссылок на зараженные и фишинговые веб-сайты .

Обеспечивает проактивную защита от неизвестных угроз, основанную на анализе поведения программ .

Обеспечивает самозащиту антивируса от попыток выключения со стороны вредоносного ПО.

Обеспечивает регулярные и экстренные обновления – всегда актуальная защита компьютера.

Kaspersky Internet Security 2013

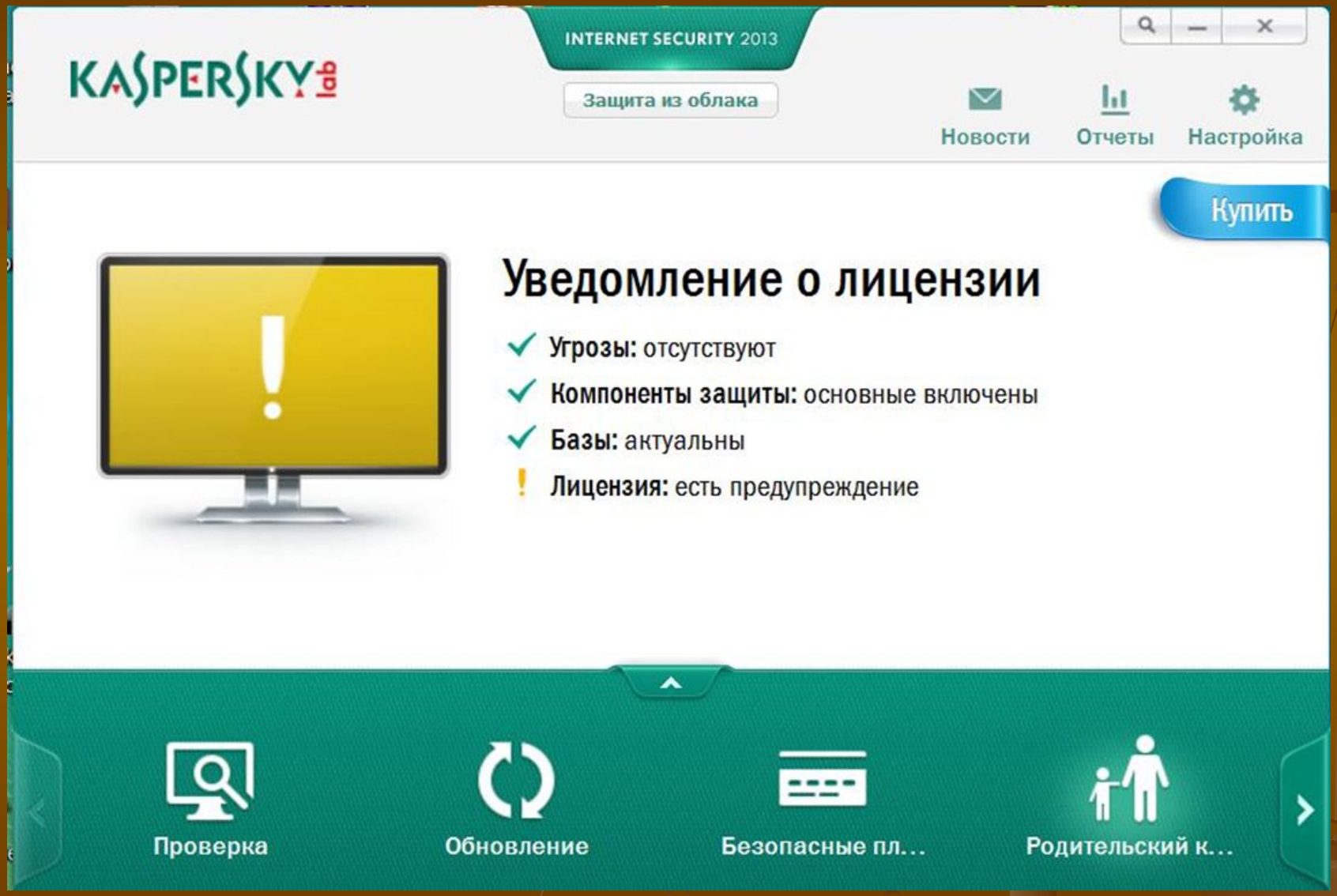
Основные функции программы

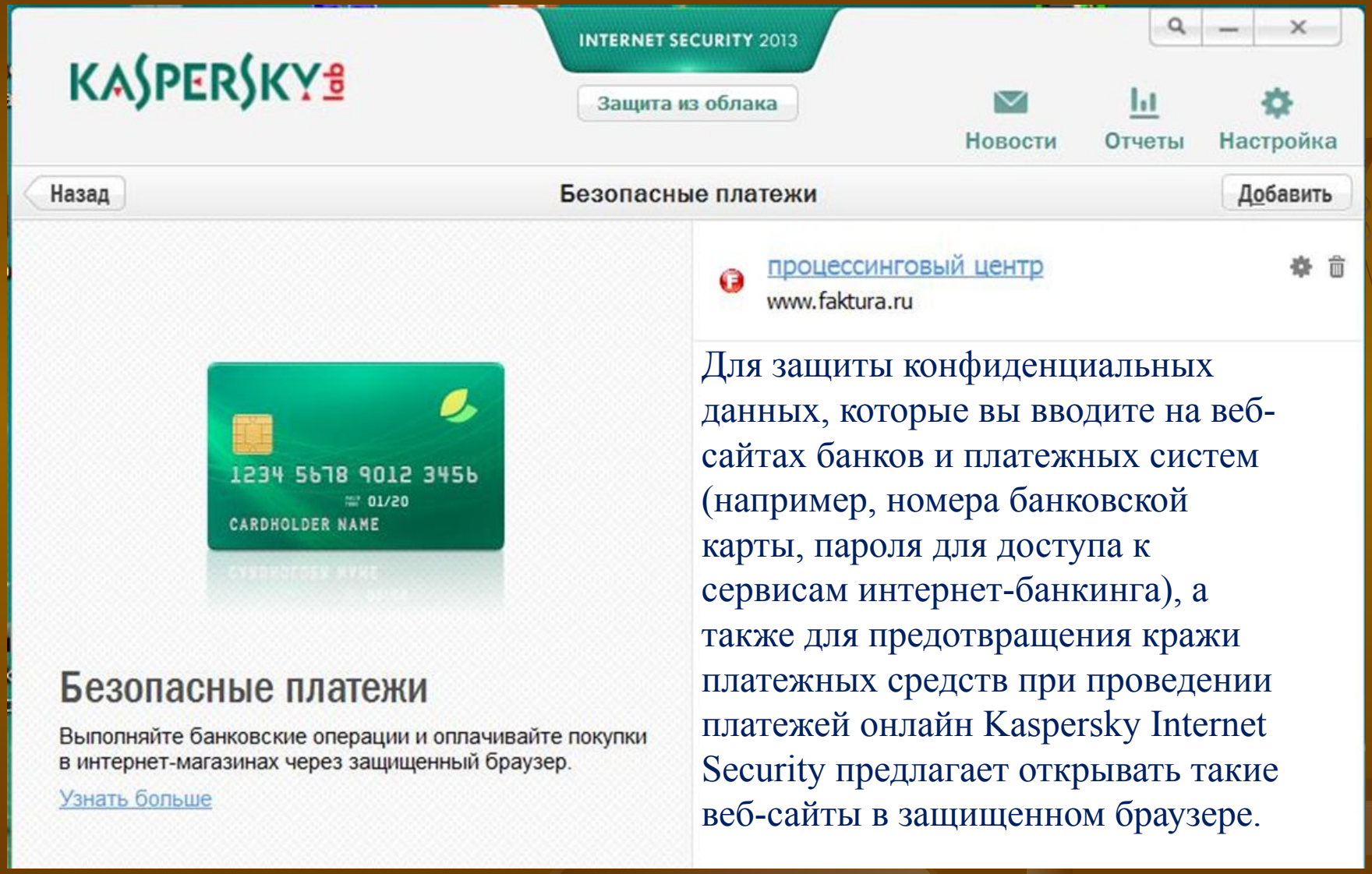
Kaspersky Internet Security обеспечивает комплексную защиту компьютера от известных и новых угроз, сетевых и мошеннических атак, спама.

Защиту компьютера в реальном времени обеспечивают следующие компоненты защиты:

- Файловый Антивирус;
- Почтовый Антивирус;
- IM-Антивирус;
- Контроль программ;
- Сетевой экран;
- Мониторинг сети;
- Защита от сетевых атак;
- Анти-Спам;
- Анти-Фишинг;
- Анти-Баннер;
- Безопасные платежи;
- Родительский контроль

Эксплойт, **эксплоит** — компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему. Целью атаки может быть как захват контроля над системой, так и нарушение её функционирования.


KASPERSKY lab
INTERNET SECURITY 2013
Защита из облака
Новости
Отчеты
Настройка
Купить
Уведомление о лицензии
Угрозы: отсутствуют
Компоненты защиты: основные включены
Базы: актуальны
Лицензия: есть предупреждение
Проверка
Обновление
Безопасные пл...
Родительский к...



Для защиты конфиденциальных данных, которые вы вводите на веб-сайтах банков и платежных систем (например, номера банковской карты, пароля для доступа к сервисам интернет-банкинга), а также для предотвращения кражи платежных средств при проведении платежей онлайн Kaspersky Internet Security предлагает открывать такие веб-сайты в защищенном браузере.

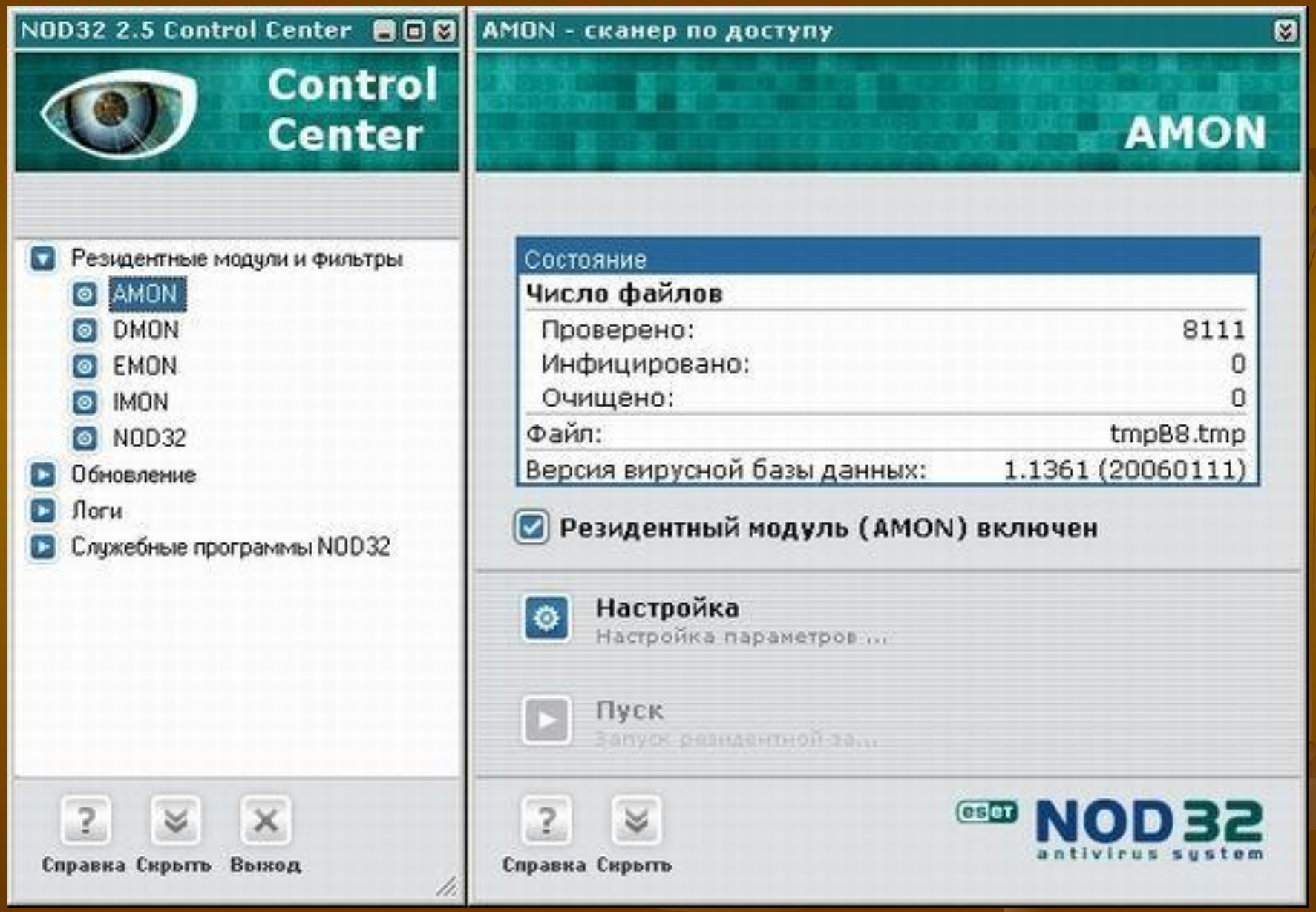
Антивирус NOD32

Антивирус NOD32 выпущен одним из лидеров антивирусного рынка, компанией ESET. За последние годы NOD32 завоевал популярность на российском рынке наряду с известными отечественными продуктами "Антивирус Касперского" и Dr.Web.

Компания Eset предоставляет различные решения, как домашние, так и многопользовательские, включающие в себя, например, серверные приложения под Linux. Приложение для конечного пользователя имеет обозначение **NOD32 Standard**.

Основой комплекса является его модульная структура именуемая **Мониторами.** Он как бы состоит из пяти частей: сканера по запросу **NOD32**, резидентного процесса **AMON**, интернет-монитора **IMON**, модуля для проверки документов Microsoft Office **DMON** и сканера электронной почты **EMON**

NOD32 | Базовые функции



Firewall

Межсетевой экран или **сетевой экран** — комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях в соответствии с заданными правилами.

Основной задачей сетевого экрана является защита компьютерных сетей или отдельных узлов от несанкционированного доступа. Также сетевые экраны часто называют фильтрами, так как их основная задача — не пропускать (фильтровать) пакеты, не подходящие под критерии, определённые в конфигурации.

В этой технологии используют также термин **Брандма́уэр.**

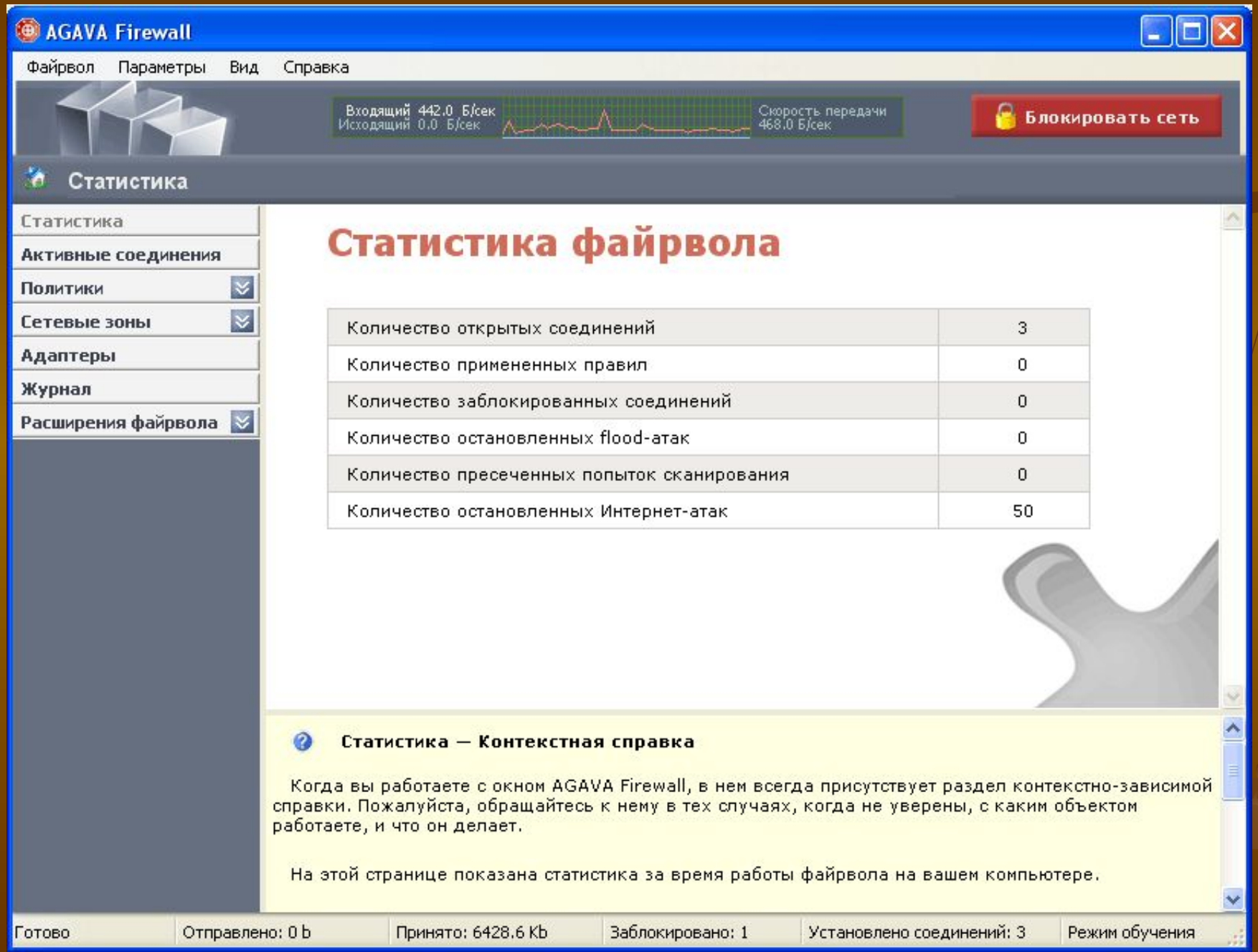
Брандма́уэр — заимствованный из немецкого языка термин, являющийся аналогом английского *firewall* в его оригинальном значении).

Опасности из сети

Приложения, созданные злоумышленниками, способны проникнуть по сети на незащищенный компьютер и запускаться незаметно для Вас. Они могут:

- Собирать и пересылать Вашу персональную информацию (реквизиты, пароли, номера кредитных карт и т.п.) своим создателям или просто удалять важные данные.
- Использовать зараженный компьютер для рассылки спама, распространения вирусов, взлома удаленных сервисов, совершения других противоправных действий.
- Генерировать большое количество паразитного трафика и делать звонки на платные телефонные номера через модем.
- Показывать рекламные окна и перенаправлять интернет-браузер на рекламные страницы.
- Подменять страницы известных сайтов на свои и использовать это для финансовых махинаций (так называемый "фишинг").
- Нарушать работу других программ и операционной системы в целом.

AGAVA Firewall

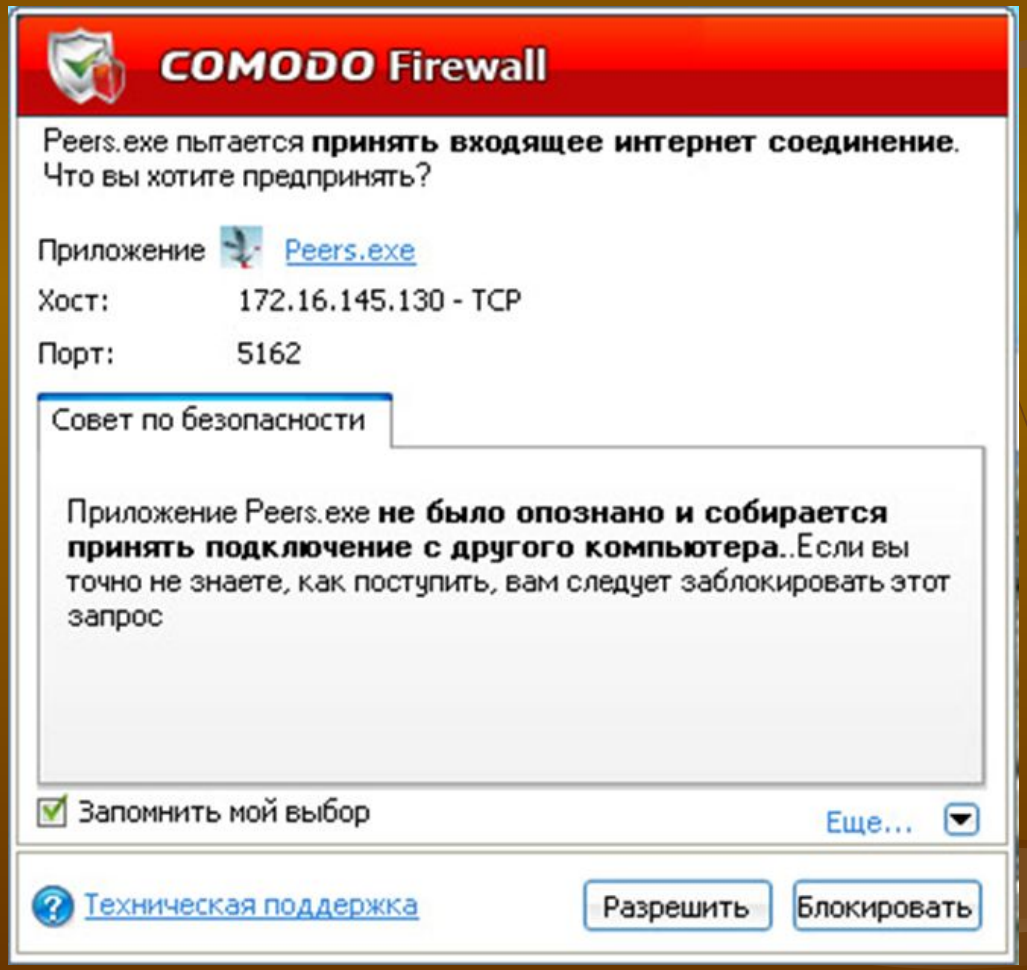


Файрвол - это программа, представляющая собой защитный барьер между компьютером и внешним миром. Хакеры используют специальное программное обеспечение для сканирования интернета и поиска незащищенных компьютеров. Такие программы посылают маленький пакет данных компьютеру. Если на компьютере нет файрвола, то он автоматически отвечает на принятое сообщение, и это означает для хакера, что система открыта и может быть взломана. Файрвол распознает такие случаи и не отвечает на подобные сообщения. Таким образом, хакеры даже не могут узнать, что компьютер подключен к сети.

Внутри локальной сети, которую от внешних угроз защищает корпоративный файрвол, рабочая станция пользователя остается беззащитной. Настройки общего файрвола не позволяют запретить активность тех приложений, которые запущены на рабочей станции, а так же предотвратить распространение вирусов. При помощи специальных типов атак злоумышленник может в локальной сети получить любые данные, которые передаются по сети с пользовательского компьютера. Переговоры по ICQ, почтовые пароли, письма и любая другая конфиденциальная информация может быть перехвачена до того, как она дойдет до получателя.


COMODO
Firewall
Comodo Internet Security
Сводка
Фаервол
Защит
Настройки
Этот раздел позволяет вам изменять общие настройки, такие как защита паролем, параметры обновления, язык, тема и т.д.
Посетить форумы поддержки
Нужна помощь? Найдите ответы на ваши во
форумах COMODO.
Управление моими конфигурациями
Этот раздел позволяет импортировать, экспортировать или удалять ваши настройки Фаервола.
Справка
Хотите узнать больше о вашем Фаерволе? В
использовать этот раздел, чтобы просмотр
справки.
Диагностика
Ваш Фаервол сообщил об ошибке? Это инструмент поможет определить проблему.
О программе
Просмотреть информацию об авторских пра
вашего Фаервола.
Проверить наличие обновлений
Проверить наличие последних обновлений, чтобы убедиться, что у вас установлена актуальная версия.

Пакет **Comodo Internet Security** (CIS) позволяет организовать надежную защиту от внешних и внутренних угроз благодаря имеющимся на вооружении мощному **Антивирусу**, **Фаерволу** корпоративного класса и высокотехнологичной подсистеме **Проактивная Защита** для предотвращения несанкционированного проникновения на уровень сервера.



Отличительной особенностью версии 4.0 является наличие **Sandbox** - нового компонента, представляющего собой изолированную среду для запуска неизвестных приложений и являющегося очередным шагом вперед на пути достижения большей безопасности и удобства в работе пользователей.