Лекция 12

28.0 **Компьютерные вирусы**

Надёжность работы компьютерных систем во многом зависит от мер самозащиты. Количество вирусов постоянно растёт, это требует от пользователя ПК знаний о природе вирусов, способов заражения и защиты от них.

Компьютерный вирус *это программный код*, встроенный в другую программу или в документ, или в определенные области носителя данных и предназначенный для выполнения несанкционированный действий на несущем компьютере.

Вирус – это программа, обладающая способностью к самовоспроизведению.

Признаки наличия вируса в работе на ПК*:*

- некоторые программы перестают работать или начинают работать неправильно;
- на экран выводятся посторонние сообщения, символы, звуковые сигналы и т.д.;
- работа на компьютере существенно замедляется;
- невозможность загрузки операционной системы;
- некоторые файлы оказываются испорченными;
- изменение размеров файлов;
- увеличение количества файлов на диске;
- частые зависания и сбои компьютера и т.д.

Пути проникновения вирусов:

- гибкие диски, flash;
- лазерные диски;
- компьютерные сети.

Заражение жесткого диска вирусами может произойти при загрузке программы с дискеты, содержащей вирус. Заразить дискету гораздо проще, достаточно вставить ее в дисковод зараженного компьютера и прочитать ее оглавление.

По прошествии некоторого времени после заражения на компьютере начинает твориться что-то странное. К этому моменту, как правило, уже достаточно много (или даже большинство) программ являются зараженными вирусом, а некоторые файлы и диски - испорченными. Более того, зараженные программы с одного компьютера могли быть перенесены с помощью flash или по локальной сети на другие компьютеры.

Некоторые виды вирусов ведут себя еще более коварно. Они вначале незаметно заражают большое число программ или дисков, а потом причиняют очень серьезные повреждения, например, форматируют весь жесткий диск на компьютере. А бывают вирусы, которые стараются вести себя как можно более незаметно, но понемногу и постепенно портят данные на жестком диске компьютера.

История компьютерной вирусологии представляется сегодня постоянной "гонкой за лидером", причем, лидерами являются именно вирусы. Среди тысяч вирусов лишь несколько десятков являются оригинальными разработками, все остальные – "вариации на тему".

Механизм заражения вирусом:

1. При запуске программы, несущей вирус, происходит запуск этого кода, что вызывает изменения в файловой системе жестких дисков и в содержании других программ. Вирус может воспроизводить себя в теле других программ. Создав достаточное количество копий, вирус может перейти к разрушительным действиям – **вирусной атаки**. Самые разрушительные вирусы могут инициировать форматирование жестких дисков.

2. При загрузке компьютера с внешнего диска, зараженного вирусом, сначала происходит проникновение вируса в оперативную память (ОП), а затем в загрузочный сектор жестких дисков. Далее этот компьютер сам становится источником распространения загрузочного вируса.

3. Результат атаки может быть как относительно безобидным, так и разрушительным.

«***Болезнь лучше предотвратить, чем лечить***». Создавать систему безопасности следует с предотвращения разрушительных последствий любого воздействия. Надежная работа с данными достигается тогда, когда любое неожиданное событие не приведёт к катастрофическим последствиям.

Причины появления и распространения компьютерных вирусов:

– с одной стороны, они скрываются в психологии человеческой личности и ее теневых сторонах (зависти, мести, тщеславии «непризнанных» творцов),

– с другой стороны, они обусловлены отсутствием аппаратных средств защиты и противодействия со стороны операционной системы персонального компьютера.

28.1 ***Классификация вирусов***

Компьютерные вирусы можно классифицировать по:

- среде обитания;
- способу заражения среды обитания;
- воздействию;
- особенностям алгоритма.

1. По среде обитания:

Сетевые – распространяются по компьютерным сетям;

Файловые – внедряются в исполняемые модули, т.е. в файлы с расширениями *.com, *.exe;

Загрузочные – внедряются в загрузочный сектор диска;

Файлово – ***загрузочные*** – заражают как файлы, так и загрузочные сектора дисков.

2. По способу заражения:

Резидентные – при заражении компьютера оставляют в ОП свою резидентную часть, которая перехватывает обращения ОС к файлам и внедряется в них.

Они являются активными до выключения или перезагрузки ПК;

Нерезидентные – не заражают память компьютера и являются активными ограниченное время.

3. По степени воздействия:

Неопасные – не мешают работе компьютера, но уменьшают объем ОП и на дисках;

Опасные – могут привести к различным нарушениям в работе компьютера;

Очень опасные – приводят к потерям программ, данных, стиранию информации в системных областях диска.

4. По особенностям алгоритма:

Паразитические – изменяют содержимое файлов и секторов диска, могут быть легко обнаружены и уничтожены;

Вирусы-репликаторы *(черви)* – распространяются по компьютерным сетям, вычисляют адреса сетевых компьютеров и записывают по этим адресам свои копии;

Вирусы-невидимки – перехватывают обращения ОС к пораженным файлам и секторам дисков и подставляют вместо своего тела незараженные участки диска. Их трудно обнаружить.

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

Основными типами компьютерных вирусов являются:

- Программные вирусы (файловые);
- Загрузочные вирусы;
- Макровирусы.

Программные вирусы – это блоки программного кода, целенаправленно внедрённые внутрь прикладных программ. Вирусный код может *размножаться.*

Поступают на компьютер при запуске непроверенных программ, полученных на внешних носителях (CD диск, гибкий диск, flash и т.п.) или принятых из Internet.

Загрузочные вирусы – поражают определённые системные области flash и жестких дисков, могут располагаться в оперативной памяти.

Заражение происходит при загрузке компьютера с носителя, системная область которого содержит загрузочный вирус.

Макровирусы – поражают документы, выполненные в некоторых прикладных программах, имеющих средства для исполнения *макрокоманд* (документы MS Word).

Заражение файла происходит при открытии файла в окне программы, если в ней не отключена возможность исполнения макрокоманд.

28.2 ***Метода защиты от компьютерных вирусов***

Существуют три рубежа защиты от вирусов:

- Предотвращение поступления вирусов;
- Предотвращения вирусной атаки;
- Предотвращение разрушительных последствий.

Существуют три метода реализации защиты:

- Программные методы защиты;
- Аппаратные методы защиты;
- Организационные методы защиты.

В случае утраты информации жесткие диски переформатируют и на «чистый» диск устанавливают ОС с компакт-диска, затем под ее управлением устанавливают все необходимое программное обеспечение, и данные с резервных носителей.

29 **Средства антивирусной защиты**

1. ***Резервное копирование*** наиболее ценных данных.

Резервные копии должны храниться отдельно от компьютера, например на удалённых серверах в Internet или на внешних носителях, которые хранятся в сейфах.

Отдельно сохранять все регистрационные и парольные данные для доступа к сетевым службам Internet. Есть службы, бесплатно предоставляющие пространство до нескольких Мбайт для хранения данных пользователя.

2. Использование ***антивирусных программ***, которые позволяют обнаружить и уничтожить вирусы.

Программные средства антивирусной защиты позволяют:

- Восстанавливать большую часть данных. В системных областях жесткого диска сохранённый образ диска может позволить восстановить большую часть данных (или все данные)
- Регулярно сканировать жесткие диски в поисках компьютерных вирусов. Сканирование происходит автоматически при каждом включении компьютера. Для надёжной работы необходимо регулярно обновлять антивирусную программу (1 раз в две недели)
- Контролировать изменение размеров и других атрибутов файлов. Вирусы на этапе размножения изменяют параметры зараженных файлов.
- Контролировать за обращением к жесткому диску. Предупреждать пользователя о подозрительной активности.

3. **Защита *носителя информации*** от записи. На некоторых Flash-ах имеется переключающий рычаг, не разрешающий запись на носитель.

29.1 **Меры по защите от вирусов**:

- Наличие современной антивирусной программы;
- Проверка носителей информации на наличие вирусов;
- Проверка принесенных файлов после разархивации;
- Периодическая проверка жестких дисков;
- Защита носителей данных от записи при работе на других ПК;
- Создание архивных копий ценных данных на дискетах;
- Не оставлять в дисководах носители данных при включении или перезагрузке ОС.

30 **Виды антивирусных программ**:

- Программы детекторы;
- Программы-доктора или фаги;
- Программы-ревизоры;
- Программы-фильтры;
- Программы-вакцины или иммунизаторы.

Программы детекторы осуществляют поиск характерной для конкретного вируса последовательности байт (сигнатуры вируса) в ОП и в файлах, и при обнаружении выдают соответствующее сообщение.

Недостаток таких антивирусных программ – возможность нахождения только тех вирусов, которые известны разработчикам таких программ.

Программы-доктора *или* ***фаги***, а также *программы-вакцины* находят зараженные вирусами файлы и лечат их, удаляя из файла тело программы вируса.

Фаги ищут тело, удаляют его, а затем "лечат" файл.

Среди фагов выделяются полифаги, т.е. программы - доктора, предназначенные для поиска и уничтожения большого количества вирусов. Поскольку постоянно появляются новые вирусы, программы-доктора устаревают и их надо регулярно обновлять.
К ним относятся: Aidstest, Scan, Norton AntiVirus, Doctor Web, AVP.

Программы-ревизоры *самые надежные средства защиты.*

Они запоминают исходное состояние программ, папок и системных областей, когда компьютер не заряжен вирусом, а затем сравнивают текущее состояние с исходным.

Изменения выводятся на экран монитора.

Сравнение состояний производят сразу после загрузки ОС. При сравнении проверяются длина файла, контрольная сумма файла, дата и время модификации и др.

К ним относятся: ADinf фирмы "Диалог-Наука".

Программы-фильтры или "***сторожа***" – резидентные программы, предназначенные для обнаружения подозрительных действий при работе компьютера, характерных для вируса, таких как:

- коррекция файлов с расширениями .com, .exe.
- изменение атрибутов файлов;
- запись в загрузочные сектора диска;
- загрузка резидентной программы.

Эти программы позволяют обнаружить вирус на ранней стадии его существования до размножения.

Для уничтожения вируса применяются фаги.

При попытке какой-либо программы произвести указанные действия "сторож" посылает пользователю сообщение и предлагает запретить или разрешить нужное действие.

Вакцины *или* ***иммунизаторы*** – это резидентные программы, предотвращающие заражение файлов. Вакцины применяют, если отсутствуют программы-доктора, "лечащие" этот вирус.

Вакцина возможна только от известных вирусов. Вакцина модифицирует программу или диск таким образом, чтобы это не отражалось на их работе, а вирус будет воспринимать их зараженными и поэтому не внедрится.

К антивирусным программам относятся:

- **AVP - Anti Viral Toolkit Pro –** профессиональный антивирусный набор (Россия),
- **Avast antivirus** - профессиональный антивирусный набор (Чехословакия),
- **Doctor Web (**Россия)**,**
- **VirusScan (**США) и другие.

Все они сходны по основным методам своей работы.

Принцип работы: Вирусы содержат характерные последовательности команд. Эти последовательности (**сигнатуры**) для известных вирусов занесены в специальные базы данных. Антивирусная программа сканирует диски, программы, файлы с целью выявления этих последовательностей для дальнейшего лечения зараженных объектов.

ЗАО “Лаборатория Касперского” - крупнейшая российская компания, производящая антивирусное программное обеспечение.

Лаборатория **Касперского** - это группа высококвалифицированных разработчиков, инженеров и менеджеров под руководством Евгения Касперского, известного специалиста по борьбе с компьютерными вирусами. AVP неоднократно, в течение нескольких лет, занимает первые места в независимых тестах антивирусных программ во всем мире.

Программа **AVP** может работать в режимах

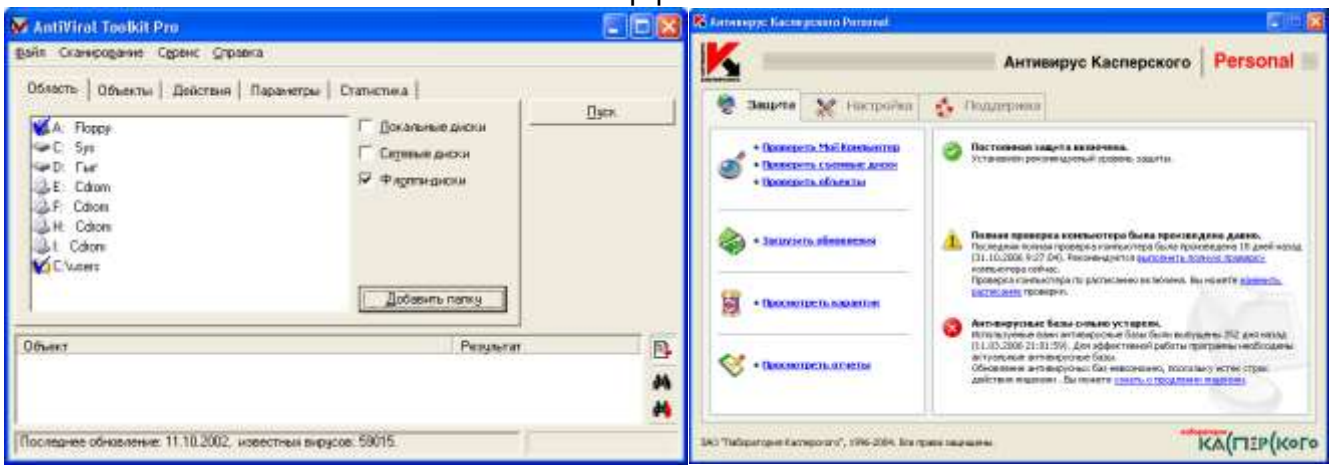
- сканера и
- монитора.

Сканеры просматривают содержимое дисков в поисках характерных последовательностей. Чтобы обнаружить новый вирус, сканеры ищут последовательности команд, могущие совершать вредные действия.

Чтобы обнаружить новый, еще неизвестный вирус, сканеры ищут последовательности команд, в принципе могущие совершать вредные действия (эвристический анализ).

Мониторы проверяют действия, которые могут выполняться вирусами, например запись в служебную область жесткого диска, перезапись файлов, проверку содержимого гибкого диска, с целью заблаговременного обнаружения вирусов.

Интерфейс AVP



Для начала поиска AVP вирусов:

1. Указать область поиска щелчком мыши по выбранному значку диска. Кнопкой «*Добавить папку*» можно задать поиск в конкретной папке на диске.
2. С помощью вкладки Объекты можно указать, в каких файлах должен выполняться поиск вирусов (в программах, в файлах).
3. Вкладка Действие позволяет задать действия, которые должен выполнить антивирус, обнаружив заражённые файлы. Этими действиями могут быть задание отчёта, лечение, полное удаление файла с диска.
4. Вкладка Параметры позволяет задать параметры программы.
5. Вкладка Статистика даёт представление о ходе поиска вирусов. На вкладке показывается, сколько файлов и папок уже проверено, сколько вирусов было найдено, вылечено, удалено.

Программа **Doctor Web**

Выполняет поиск и удаление известных ему вирусов из памяти и с дисков компьютера. Программа осуществляет эврестический анализ файлов и системных областей дисков компьютера. Разрабатывается компанией Доктор Веб

Эврестический анализ позволяет обнаружить новые, ранее неизвестные вирусы.

Dr. Web — семейство антивирусов, предназначенных для защиты
от почтовых и сетевых червей,
файловых вирусов,
троянских программ,
стелс-вирусов,
полиморфных вирусов,
бестелесных вирусов,
макровирусов,
вирусов, поражающих документы MS Office,
скрипт-вирусов,
шпионского ПО (spyware),
программ-похитителей паролей,
клавиатурных шпионов,
программ платного дозвона,
рекламного ПО (adware),
потенциально опасного ПО,
хакерских утилит,
программ-люков,
программ-шуток,
вредоносных скриптов и
других вредоносных объектов,
а также от спама, и технического спама.

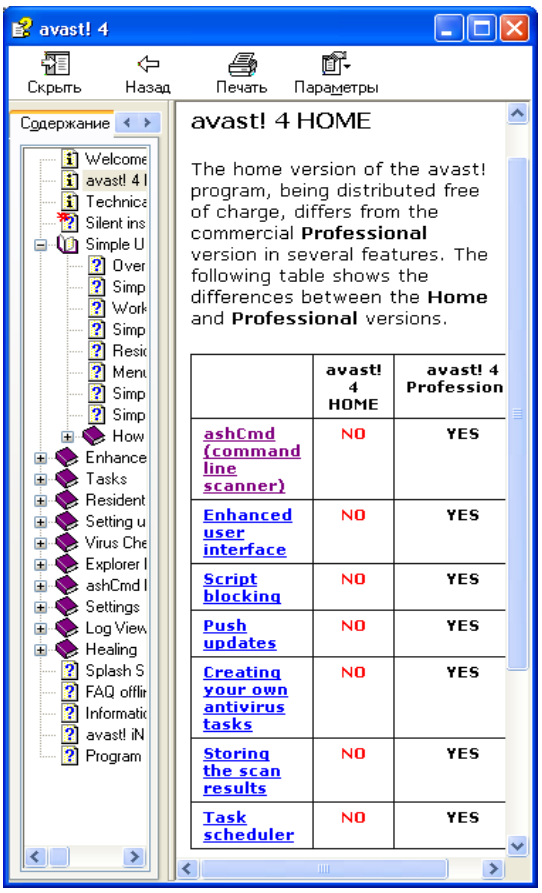
Кнопки панели инструментов:

1. Список отчета
2. Дерево дисков
3. Статистика
4. Очистить список отчета
5. Обновить DrWeb через Internet
6. Установки
7. Выход

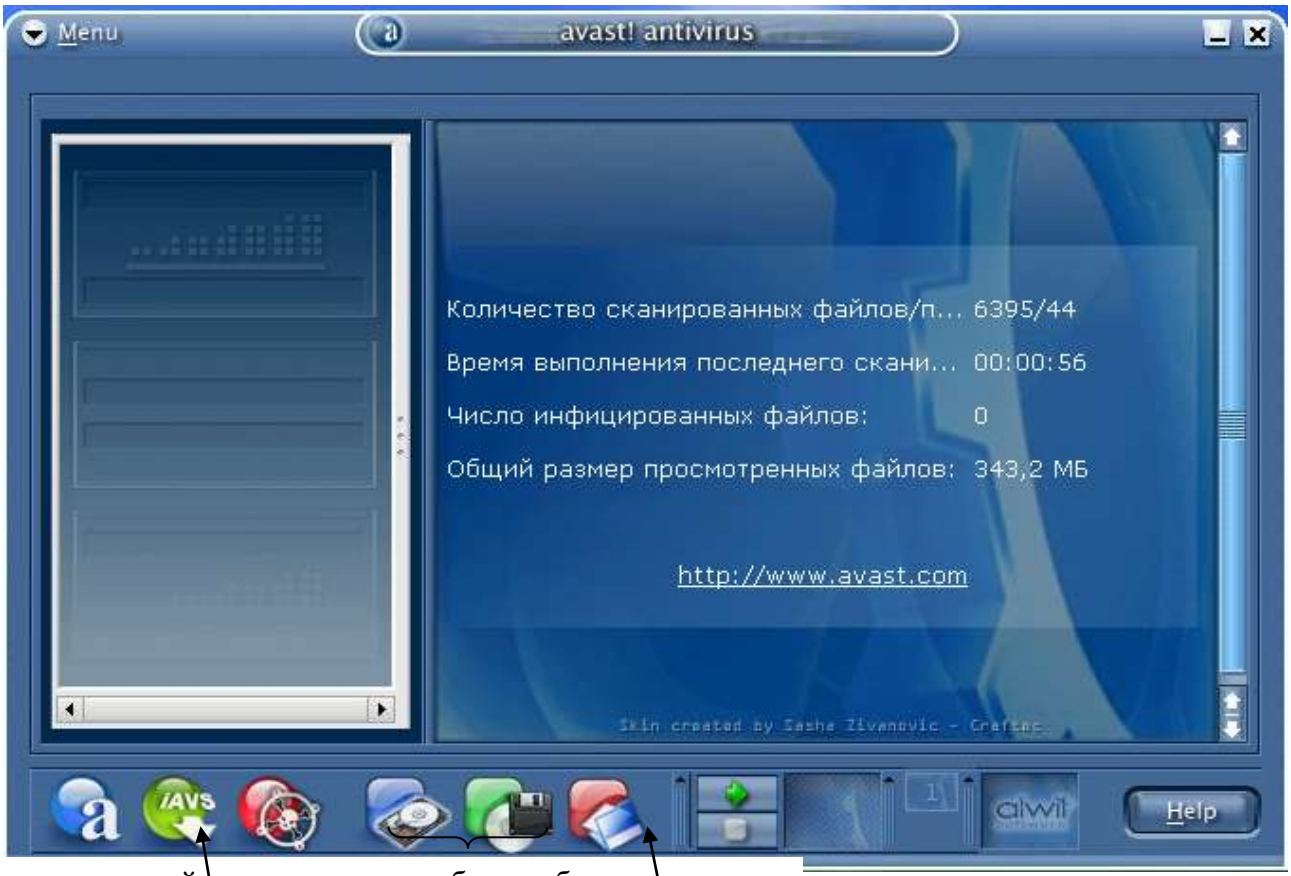
После запуска антивирусной программы, прежде всего, производят ее настройку.

Проверяемая папка выбирается на дереве папок в главном окне программы. Для отображения на дереве папок файлов, необходимо установить флаг *Файлы в дереве.*

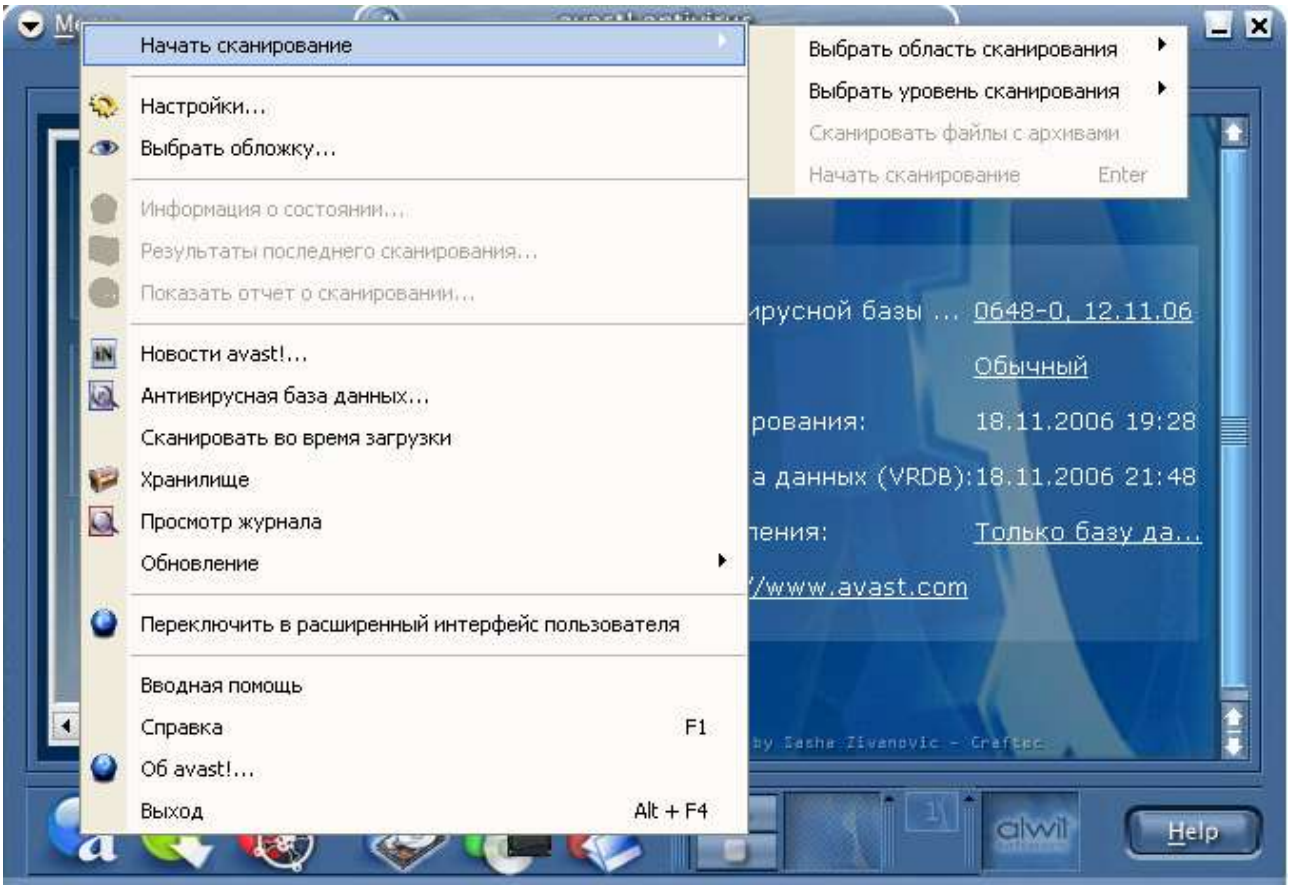
Программа **avast**



Интерфейс **avast**



резидентный сканер | обновление | хранилище локал./ съемных дисков | выбор области сканирования | запуск



Интерфейс программы Avast (последняя версия)