# 14. ОСНОВЫ БОРЬБЫ С ВРЕДОНОСТНЫМИ ПРОГРАММАМИ

## *14.1 Самостоятельная диагностика заражения вредоносными программами*

### 14.1.1 Признаки и диагностика заражений через браузер

Явные проявления обычно заражений через Браузер выражаются в неожиданно появляющихся рекламных сообщениях и баннерах - обычно это следствие проникновения на компьютер рекламной утилиты. Поскольку их главная цель - это привлечь внимание пользователя к рекламируемой услуге или товару, то им сложно оставаться незаметными. Также явные проявления могут вызывать ряд троянских программ, например утилиты несанкционированного дозвона к платным сервисам. Они вынуждены быть явными, поскольку используемые ими приложения сложно использовать незаметно от пользователя.

### 14.1.2 Подозрительные процессы

Одним из основных проявлений вредоносных программ является наличие в списке запущенных процессов (в ОС семейства Windows вызывается через CTRL+ALT+DEL, рис 14.1) подозрительных программ. Исследуя этот список и особенно сравнивая его с перечнем процессов, которые были запущены на компьютере сразу после установки системы, то есть до начала работы, можно сделать достаточно достоверные выводы об инфицировании. Это часто помогает при обнаружении вредоносных программ, имеющих лишь только скрытые или косвенные проявления.

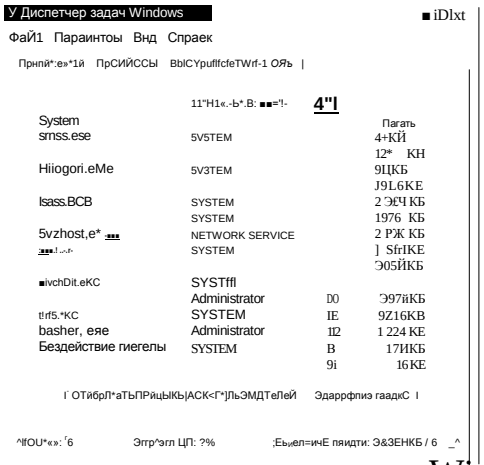


Рис. 14.1 – Просмотр запущенных в системе Windows процессов

### 14.1.3 Сетевая активность

Неожиданно возросшая сетевая активность может служить ярким свидетельством работы на компьютере подозрительный программы. Но при этом нужно не забывать, что ряд вполне легальных приложений также имеют свойство иногда связываться с сайтом фирмы-производителя, например для проверки наличия обновлений или более новых версий. Поэтому, прежде чем отключать сеть необходимо уметь определять какие программы и приложения вызвали эту подозрительную активность.

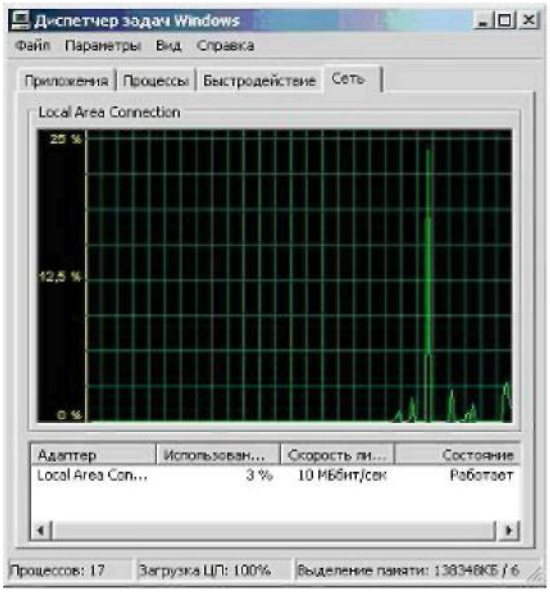


Рис. 14.2

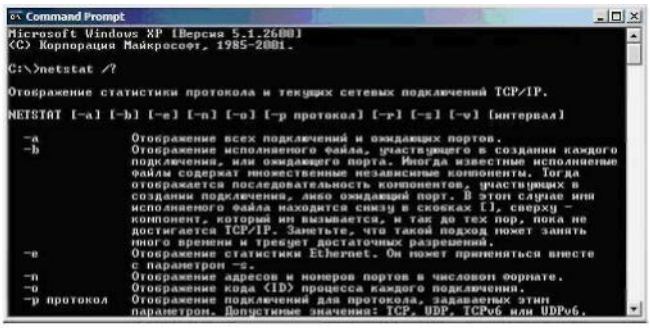


Рис. 14.3

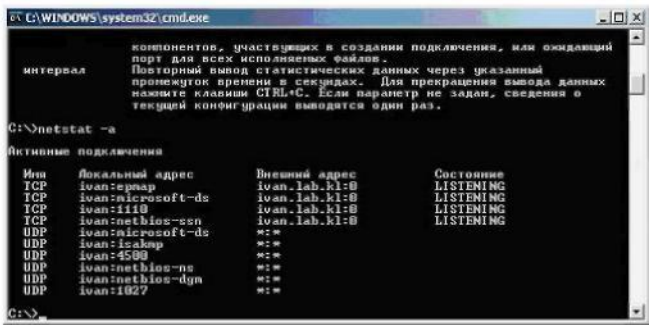


Рис. 14.4

Изучить и проанализировать сетевую активность можно с помощью встроенных в операционную систему инструментов или же воспользовавшись специальными отдельно устанавливаемыми приложениями. В этом задании это предлагается сделать с помощью **Диспетчера задач Windows** (рис. 14.2) и встроенной утилиты netstat (рис. 14.3, 14.4), которая выводит на экран мгновенную статистику сетевых соединений.

### 14.1.4 Элементы автозапуска

Для того, чтобы прикладная программа начала выполняться, ее нужно запустить. Следовательно, и вирус нуждается в том, чтобы его запустили.

Оптимальным с точки зрения вируса вариантом служит запуск одновременно с операционной системой - в этом случае запуск практически гарантирован.

Вредоносная программа может вносить изменения в системные файлы win.ini и system.ini.

Следует также отметить, что в файле system.ini кроме секции [boot] вредоносные программы могут использовать секцию [Drivers].

Вредоносные программы могут вносить изменения в следующие ветки реестра:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion в ключи Run, RunOnce, RunOnceEx, RunServices, RunServicesOnce - для того чтобы система запускала созданные червем файлы
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion в ключ Run.

Кроме выше перечисленных ветвей и ключей реестра вредоносные программы могут вносить изменения и в другие ветки и ключи реестра, например:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\WOW\boot
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\Drivers32
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\ CurrentVersion\WinLogon
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\ Installed Components
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\AeDebug

Диагностика элементов автозапуска возможно путем изучения секций: SYSTEM.INI (рис. 14.5); WIN.INI (рис. 14.6); «Автозапуск» (рис. 14.7) и «Службы» (рис. 14.8), в утилите конфигурирования msconfig. Удаление запускаемого вируса из автозагрузке возможно путем использования утилиты regedit.

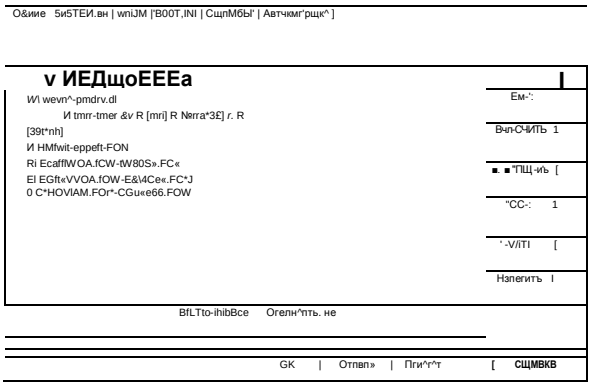


Рис. 14.5

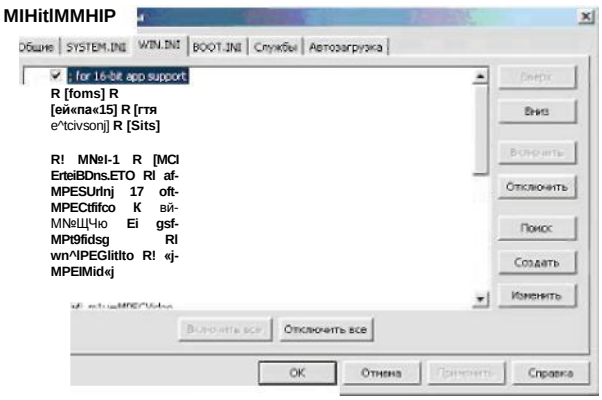


Рис. 14.6

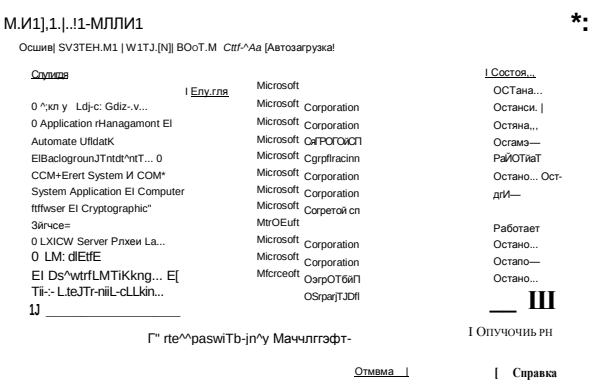


Рис. 14.7

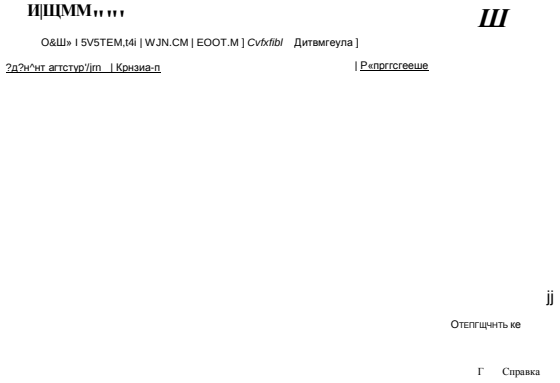


Рис. 14.8

## *14.2 Основы функционирования антивирусного программного обеспечения*

***Антивирус*** *- программное средство, предназначенное для борьбы с вирусами.*

***Основными задачами антивируса является:***

- *Препятствование проникновению вирусов в компьютерную систему.*
- *Обнаружение наличия вирусов в компьютерной системе.*
- *Устранение вирусов из компьютерной системы без нанесения повреждений другим объектам системы. Минимизация ущерба от*
- *действий вирусов.*

### 14.2.1 Технологии обнаружения вирусов

***Технологии, применяемые в антивирусах, можно разбить на две группы***

1. *Технологии сигнатурного анализа.*
2. *Технологии вероятностного анализа:*
   - *2.1. Эвристический анализ.*
   - *2.2. Поведенческий анализ.*
   - *2.3. Анализ контрольных сумм.*

***Сигнатурный анализ*** *- метод обнаружения вирусов, заключающийся в проверке наличия в файлах сигнатур вирусов.* Сигнатурный анализ является наиболее известным методом обнаружения вирусов и используется практически во всех современных антивирусах. Для проведения проверки антивирусу необходим набор вирусных сигнатур, который хранится в антивирусной базе. Ввиду того, что сигнатурный анализ предполагает проверку файлов на наличие сигнатур вирусов, антивирусная база нуждается в периодическом обновлении для поддержания актуальности антивируса.

***Недостатки сигнатурного анализа*** *определяют границы его функциональности - возможность обнаруживать лишь уже известные вирусы - против новых вирусов сигнатурный сканер бессилен.*

***Достоинством сигнатурного анализа*** *является то, что наличие сигнатур вирусов предполагает возможность лечения инфицированных файлов, обнаруженных при помощи сигнатурного анализа.* Однако, лечение допустимо не для всех вирусов - трояны и большинство червей не поддаются лечению по своим конструктивным особенностям, поскольку являются цельными модулями, созданными для нанесения ущерба. Грамотная реализация вирусной сигнатуры позволяет обнаруживать известные вирусы со стопроцентной вероятностью.

***Эвристический анализ*** *- технология, основанная на вероятностных алгоритмах, результатом работы которых является выявление подозрительных объектов. В процессе эвристического анализа проверяется структура файла, его соответствие вирусным шаблонам.* Наиболее популярной эвристической технологией является проверка содержимого файла на предмет наличия модификаций уже известных сигнатур вирусов и их комбинаций. ***Достоинством эвристического анализа*** *является то, что он может определять гибриды и новые версии ранее известных вирусов без дополнительного обновления антивирусной базы.* ***Недостатком*** *– то, что эвристический анализ не предполагает лечения.* Данная технология не способна на 100% определить вирус перед ней или нет, и как любой вероятностный алгоритм грешит ложными срабатываниями.

***Поведенческий анализ*** *- технология, в которой решение о характере проверяемого объекта принимается на основе анализа выполняемых им операций. Поведенческий анализ весьма узко применим на практике, так как большинство действий, характерных для вирусов, могут выполняться и обычными приложениями.* Наибольшую известность получили поведенческие анализаторы скриптов и макросов, поскольку соответствующие вирусы практически всегда выполняют ряд однотипных действий. Помимо этого поведенческие анализаторы могут отслеживать попытки прямого доступа к файлам, внесение изменений в загрузочную запись дискет, форматирование жестких дисков и т. д. Поведенческие анализаторы не используют для работы дополнительных объектов, подобных вирусным базам и, как следствие, неспособны различать известные и неизвестные вирусы - все подозрительные программы априори считаются неизвестными вирусами. Аналогично, особенности работы средств, реализующих технологии поведенческого анализа, не предполагают лечения.

**Например**, средства защиты, вшиваемые в BIOS, также можно отнести к поведенческим анализаторам. При попытке внести изменения в MBR компьютера, анализатор блокирует действие и выводит соответствующее уведомление пользователю.

***Анализ контрольных сумм*** *- это способ отслеживания изменений в объектах компьютерной системы. На основании анализа характера изменений - одновременность, массовость, идентичные изменения длин файлов - можно делать вывод о заражении системы.* Анализаторы контрольных сумм (также используется название «ревизоры изменений») как и поведенческие анализаторы не используют в работе дополнительные объекты и выдают вердикт о наличии вируса в системе исключительно методом экспертной оценки. Чаще подобные технологии применяются в сканерах при доступе - при первой проверке с файла снимается контрольная сумма и помещается в кэше, перед следующей проверкой того же файла сумма снимается еще раз, сравнивается, и в случае отсутствия изменений файл считается незараженным.

### 14.2.2 Классификация антивирусного программного обеспечения

Помимо используемых технологий, антивирусы отличаются друг от друга условиями эксплуатации. Уже из анализа задач можно сделать вывод о том, что препятствование проникновению вредоносного кода должно осуществляться непрерывно, тогда как обнаружение вредоносного кода в существующей системе - скорее разовое мероприятие. Следовательно, средства, решающие эти две задачи должны функционировать по-разному.

***Таким образом, антивирусы можно разделить на две большие категории:***

- ***Предназначенные для непрерывной работы*** - к этой категории относятся средства проверки при доступе, почтовые фильтры, системы сканирования проходящего трафика Интернет, другие средства, сканирующие потоки данных.
- ***Предназначенные для периодического запуска*** - различного рода средства проверки по запросу, предназначенные для однократного сканирования определенных объектов. К таким средствам можно отнести сканер по требованию файловой системы в антивирусном комплексе для рабочей станции, сканер по требованию почтовых ящиков и общих папок в антивирусном комплексе для почтовой системы (в частности, для Microsoft Exchange).

***Антивирусный комплекс*** *- набор антивирусов, использующих одинаковое антивирусное ядро или ядра, предназначенный для решения практических проблем по обеспечению антивирусной безопасности компьютерных систем.* В антивирусный комплекс также в обязательном порядке входят средства обновления антивирусных баз.

***Антивирусное ядро*** *- реализация механизма сигнатурного сканирования и эвристического анализа на основе имеющихся сигнатур вирусов.*

***Исходя из текущей необходимости в средствах защиты выделяют следующие типы антивирусных комплексов:***

1. ***Антивирусный комплекс для защиты рабочих станций*** - *предназначен для обеспечения антивирусной защиты рабочей станции*, на которой он установлен. Состоит, как и указывалось ранее из средств непрерывной работы и предназначенных для периодического запуска, а также средств обновления антивирусных баз.
2. ***Антивирусный комплекс для защиты файловых серверов*** -*предназначен для обеспечения антивирусной защиты сервера, на котором установлен.* Указание на файловый сервер в названии является скорее данью истории, корректней будет звучать термин «сетевой». Определение того, насколько нуждается в антивирусной защите сервер, осуществляется не только исходя из его назначения (является сервер файловым, почтовым, либо выполняет другую функцию), а и из используемой на нем платформы.
3. ***Антивирусный комплекс для защиты почтовых систем****, назаначение комплекса назначение - препятствовать доставке зараженных сообщений пользователям сети, но он не предназначен для защиты почтовой системы от поражения вирусами*. Как уже указывалось ранее, сегодня одним из главных средств доставки вирусов в локальную сеть является именно электронная почта. Поэтому, при наличии в локальной сети специализированного узла, обрабатывающего входящую и исходящую из сети почтовую корреспонденцию (почтового сервера), логично будет использовать средство централизованной проверки всего почтового потока на наличие вирусов)
4. ***Антивирусный комплекс для защиты шлюзов*** - *предназначен для проверки на наличие вирусов данных, через этот шлюз передаваемых. Как правило в его состав входят:*
   - *4.1.* ***Сканер HTTP-потока*** *— предназначен для проверки данных, передаваемых через шлюз по протоколу HTTP.*
   - *4.2.* ***Сканер FTP-потока*** *— предназначен для проверки данных, передаваемых через шлюз по протоколу FTP. В случае использования FTP over HTTP FTP-запросы будут проверяться сканером HTTP-потока.*
   - *4.3.* ***Сканер SMTP-потока*** *— предназначен для проверки данных, передаваемых через шлюз по SMTP.*

## *14.3 Комплексые средства антивирусной зашиты*

### 14.3.1 Комплексы антивирусной зашиты для сетевых шлюзов

***Задача антивируса установленного на шлюзе*** *— не допустить проникновения вирусов вовнутрь сети через поток данных Интернет.*

*Существующие реализации универсальных антивирусов для шлюзов позволяют проверять данные, поступающие по следующим протоколам:*

- *HTTP;*
- *FTP;*
- *SMTP.*

***Требования к антивирусам для шлюзов:***

1. ***Основные требования*** - являющиеся по сути требованием, выполнения антивирусом свою основной задачи:
   1.1. *Проверка Интернет-потоков данных (HTTP, FTP и, возможно, SMTP)* на наличие вирусов и предотвращать проникновение вирусов в сеть.
   1.2. *Проверка составных объектов* - архивов, самораспаковывающиеся архивов, упакованных исполняемых файлоа, почтовых баз, файлов почтовых форматов.
   1.3. *Возможность настраивать действия, которые будут выполняться при обнаружении вредоносных программ в потоках данных*. Стандартными действиями при этом являются - пропустить, удалить, поместить на карантин.
   1.4. *Возможность лечениять зараженных объектов*.
2. ***Требования к управлению****:*
   2.1. *Масштабируемость* — настройки одного сервера должны легко распространяться на другие сервера или группу серверов, особенно если речь идет о массивах серверов Microsoft ISA Server или подобных решениях.
   2.2. *Удаленное управление* — администратор антивирусной безопасности должен иметь возможность управлять всеми антивирусными средствами непосредственно со своего рабочего места.

*При проверке протоколов Интернет, сервер антивирусной проверки наиболее оптимально устанавливать перед прокси-сервером, но за брандмауэром, если смотреть со стороны защищаемой сети* (рис. 14.9). Впрочем, брандмауэр может и отсутствовать. В этом случае антивирус получает на вход тот же поток, который до этого получал прокси-сервер, выполняет проверку поступающих данных на наличие вредоносного кода и передает уже проверенные данные на прокси-сервер.


Рис. 14.9 - Установка сервера антивирусной проверки перед прокси-сервером

### 14.3.2 Комплексы антивирусной защиты почтовых систем

В силу того, что по разным оценкам от 80 до 95 процентов вирусов проникает в корпоративные сети через электронную почту, проверка почтового трафика является одной из важнейших задач обеспечения антивирусной безопасности организации. При этом под почтовым трафиком понимается SMTP-поток. Антивирусные комплексы для защиты почтовых систем не проверяют данные, передаваемые по протоколам IMAP и POP при обращении пользователей к своим персональным внешним по отношению к организации ящикам, поскольку это - задача антивирусного комплекса для защиты рабочих станций. Задачей антивирусного комплекса для почтовой системы является проверка и всего потока писем, поступающих и исходящих из почтовой системы организации.

**К почтовому антивирусному комплексу, предьявляются требования, удовлетворение которых существенно упрощает задачу защиты организации от проникновения вирусов через почтовый поток:**

1. **Карантин** — кроме удаления и доставки пользователю сообщения, возможна реализация карантинного хранилища - в этом случае пользователю доставляется уведомление со ссылкой на место в карантине, где хранится вложение к его письму.
2. **Добавление информации о проверке в письмо** — в конец проверенного письма, либо в служебный заголовок добавляется

информация о том, что письмо было проверено, а также статус проверки. Указание в таком сообщении версии использованных антивирусных баз, а также точного времени проверки позволит существенно упростить служебные расследования при поражении вирусами узлов сети.

3. **Генерация списка обнаруживаемых вирусов** — может пригодиться для точного определения состояния антивирусного комплекса во время проведения служебного расследования, при условии реализации предыдущего пункта
4. **Возможность выделения различных групп пользователей и задания различных настроек проверки для этих групп** — логичное продолжение требования к возможности исключения пользователей из проверки. Некоторые пользователи, наоборот, могут входить в группу риска, поскольку обрабатывают информацию, составляющую коммерческую либо государственную тайну. Требования к проверке корреспонденции таких пользователей должны быть более жесткими чем обычные.
5. **Возможность модификации уведомлений, в том числе и для различных групп пользователей** — может пригодиться для указания адресов и телефонов, по которым нужно обращаться с вопросами касательно антивирусной защиты.
6. **Возможность блокировки объектов, не прошедших проверку** — в некоторых случаях проверить вложение на наличие вирусов не представляется возможным — к примеру, если это часть многотомного архива либо архив, защищенный паролем. В этом случае антивирусный комплекс должен обладать возможностью блокировать сообщения, содержащие подобные вложения.
7. **Вирусная атака** — при обнаружении $N$ вирусов в $M$ минут иногда полезно уведомить администратора об этом факте. Подобное поведение продукта скорее всего будет свидетельствовать о вирусной эпидемии либо атаке на сервер. В обоих случаях администратор может попытаться внести изменения в настройки самого комплекса с тем, чтобы отсеивать зараженные письма на более раннем этапе, снижая, тем самым, нагрузку на сервер

Примером антивирусной защиты для почтовых систем может являться VS API 2.0 для Microsoft Exchange Server 2000. Общая схема работы VS API 2.0 приведена на рис. 14.10.

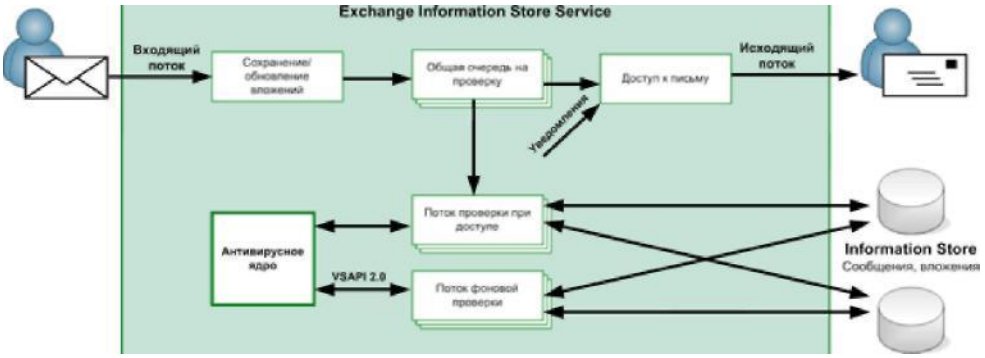


Рис. 14.10 - Схема работы VS API 2.0

### 14.3.4 Системы централизованного управления антивирусной защитой

Для локальной сети, больше количкство компьютеров, использование системы удаленного централизованного управления антивирусной защитой оказывается максимльно эффективным. Она позволяет администратору на своем рабочем месте обслуживать все рабочие станции и сервера сети:

1. возможность осуществлять полный контроль за вирусной активностью и состоянием антивирусной защиты в сети (основное преимущество),
2. быстро обнаруживать и оперативно устраненять все вирусные инцидентов,
3. удаленно настраивать политики антивирусной безопасности,
4. запускать проверку объектов на наличие в них вирусов,
5. включать или выключать постоянную защиту,
6. централизованно обновлять антивирусные базы,
7. разрешать или запрещать пользователям самим менять какие-либо настройки, в том числе позволять или не позволять им видеть, что на компьютере вообще установлен и работает антивирус.

**Система удаленного централизованного управления обычно состоит из таких отдельных программных компонентов:**

- **Клиентской антивирусной программы**, то есть антивирусного комплекса для рабочих станций или сетевых серверов.
- **Сервера администрирования** - так называется программа, которая собирает, обрабатывает и хранит все настройки, информацию обо всех событиях и инцидентах, имевших место в сети, рассылает уведомления и отчеты. Для полноценного функционирования ведется база данных для хранения всей собранной информации. Сервер администрирования и база данных могут устанавливаться как на отдельном выделенном для этого компьютере, так и на рабочем месте администратора, на одной машине или на разных.
- **Агента администрирования**, который устанавливается на все компьютеры, входящие в логическую сеть системы антивирусной

защиты. Его задача - обеспечить связь клиентской программы с сервером администрирования и оперативно передать ему информацию о состоянии антивирусной защиты на этой машине, получить новые антивирусные базы или другие указания и команды.

- **Консоли администрирования**, устанавливаемой на рабочем месте администратора. Это небольшая программа, которая позволяет в вывести данные с сервера администрирования, на их основе создать отчеты, произвести настройку клиентских компьютеров, удаленно запустить проверку или обновить антивирусные базы одновременно на нескольких машинах. Возможности той или иной консоли полностью зависят от заложенных в нее фирмой-производителем функций.

На рис. 14.11 представлена схема взаимодействия перечисленных компонентов, а на рис. 14.12 - схема сбора и передачи на хранение серверу администрирования данных о состоянии антивирусной защиты.

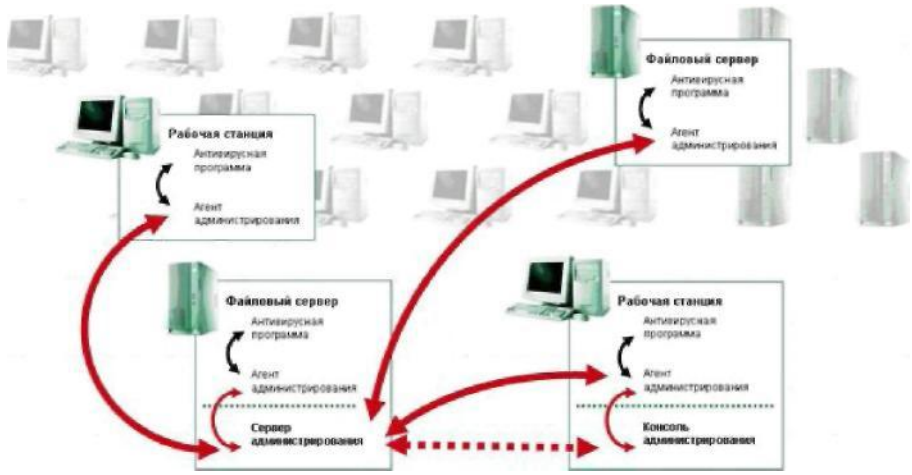


Рис. 14.11 - Схема взаимодействия компонентов централизованно управляемого комплекса антивирусной защиты в сети

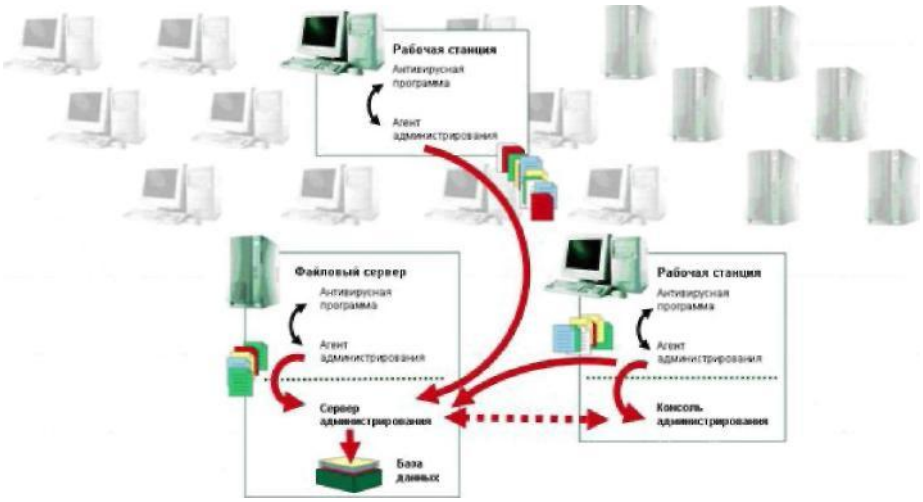


Рис. 14.12 - Схема сбора статистики в системе антивирусной защиты