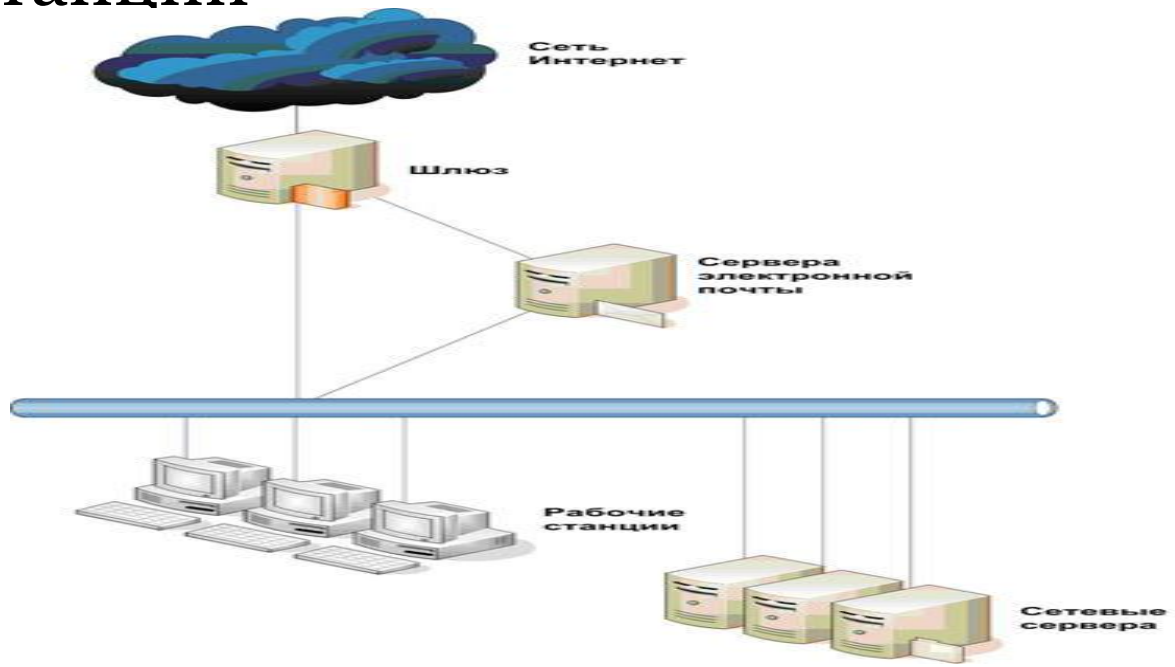
Борьба с вредоносным ПО в локальной сети

- *Проблема эпидемии сетевых червей актуальна для любой локальной сети. Рано или поздно может возникнуть ситуация, когда в ЛВС проникает сетевой или почтовый червь, который не детектируется применяемым антивирусом. Сетевой вирус распространяется по ЛВС через не закрытые на момент заражения уязвимости операционной системы или через доступные для записи общие ресурсы. Почтовый вирус, как следует из названия, распространяется по электронной почте при условии, что он не блокируется клиентским антивирусом и антивирусом на почтовом сервере. Кроме того, эпидемия в ЛВС может быть организована изнутри в результате деятельности инсайдера*

Антивирусная защита сети

- **Основы построения локальной компьютерной сети**
- Для организации полноценной и эффективной работы локальной компьютерной сети, необходимо, чтобы компьютеры в ней:
- имели возможность обмениваться информацией между собой с помощью сетевых технологий (то есть не только мобильных носителей);
- могли хранить и обрабатывать информацию на выделенных сетевых серверах, если это требуется в работе;
- получать и отправлять электронные письма;
- имели доступ в Интернет, если это предусмотрено и разрешено политикой организации;
- могли использовать другие сетевые технологии – сетевой принтер, факс.

- Большинство существующих сегодня в мире компьютерных сетей – это сети среднего масштаба, имеющие в своем составе один шлюз, который отвечает за связь с Интернет, один почтовый сервер, принимающий и пересылающий электронные письма, несколько сетевых серверов и десятки рабочих станций



Уровни антивирусной защиты

- Архитектура системы антивирусной защиты сильно зависит от функции рассматриваемого компьютера, а именно от присутствующих у него каналов связи с окружающим миром. Выделим соответствующие уровни антивирусной защиты:
- уровень защиты рабочих станций и сетевых серверов;
- уровень защиты почтовых серверов;
- уровень защиты шлюзов.
- В этой классификации на каждый почтовый сервер могут быть установлены одновременно программы, реализующие уровень защиты рабочих станций и сетевых серверов и программы, относящиеся к уровню защиты почтовых серверов. Аналогично дело обстоит и со шлюзами – программное обеспечение уровня рабочих станций и сетевых серверов и уровня защиты шлюзов.

- **Уровень защиты рабочих станций и сетевых серверов**
  Уровень защиты рабочих станций и сетевых серверов охватывает все компьютеры локальной сети и служит самым последним оплотом на пути проникновения вредоносных программ. Даже если где-то в системе антивирусной защиты случился прокол, и одна машина все же оказалась заражена, установленные на остальных компьютерах антивирусные программы должны предотвратить дальнейшее распространение эпидемии по сети.
  Защита рабочих станций и сетевых серверов ответственна в первую очередь за чистоту файловой системы каждого из компьютеров сети. Следовательно, она в обязательном порядке должна содержать постоянную проверку, как механизм предотвращения заражения системы вирусами, проверку по требованию – процедуру для тщательной ревизии рассматриваемой машины, и нейтрализации проникших на нее вредоносных программ, и модуль для поддержания вирусных сигнатур в актуальном состоянии.
  С помощью специальных программ и утилит для централизованного удаленного управления, можно не вставая из-за своего компьютера одновременно управлять и настраивать программы на удаленных компьютерах и подчиненных ему других элементах сети.
  Следовательно, к антивирусному комплексу для защиты рабочих станций и сетевых серверов предъявляется дополнительное требование – наличие в его составе программного средства для удаленного централизованного управления локальными приложениями.

- **Уровень защиты почты**

Это вторая ступень в антивирусной защите сети, и служит для уменьшения нагрузки и увеличения надежности системы защиты рабочих станций и сетевых серверов. Антивирусная проверка исходящей корреспонденции, в случае одиночного вирусного инцидента внутри сети послужит преградой для распространения этого вируса на другие, внешние, компьютеры. В системе защиты этого уровня используется комплекс для защиты почтовых систем.

Почтовый сервер – это компьютер, на котором установлена и успешно функционирует программа по обработке почты. Почтовый сервер относится к серверной группе, а не к рабочим станциям, т.к. его главное предназначение состоит в обеспечении работы почтовой системы, а не в решении локальных прикладных задач. А значит, почтовый сервер фактически представляет собой хранилище информации (электронных писем) для других сетевых пользователей. Почтовая программа или агент пересылки сообщений осуществляет передачу электронных писем от одного компьютера к другому. Т.е. компьютер отправителя, который находится во внутренней сети, связывается с почтовой программой на сервере и пересылает ей письмо, который выделяет из письма адрес получателя и производит дальнейшее перенаправление – в Интернет или обратно в локальную сеть другому пользователю из нее. Почтовый агент уведомляет пользователя, что у него в ящике появилось новое сообщение. Если он захочет его получить, то почтовый агент связывается с сервером и копирует файлы письма на машину пользователя. Таким образом, на сервере образуется очередь из еще не отосланных и еще неполученных писем, а также полностью или частично хранится входящая корреспонденция.

Поэтому антивирусная проверка должна включать в себя, как проверку всех проходящих через почтовую программу потоков, так и хранилища электронных писем.

- Антивирусный комплекс для защиты почты должен содержать:
- антивирусную проверку в режиме реального времени проходящей через почтовую систему корреспонденции;
- антивирусную проверку в режиме реального времени файлов, запрашиваемых пользователями из своих почтовых ящиков;
- антивирусную проверку по требованию для хранимых на сервере файлов почтового формата, а именно информации в ящиках пользователей;
- средство для обновления антивирусных баз.
- **Уровень защиты шлюзов**
  Антивирусная защита на уровне шлюза играет вспомогательную роль в общей системе антивирусной безопасности сети, т.к. задача такого антивирусного комплекса – только проверка поступающей извне информации на наличие в ней вредоносных программ. Однако даже если вирус проникнет сквозь шлюз, заразить ни один компьютер ему не удастся: его перехватит антивирус на локальной машине, а в случае инфицированного почтового сообщения – он будет остановлен еще на почтовом сервере.
  Шлюз – это компьютер с установленной программой, реализующий механизм передачи данных от одной сети к другой. Обычно под этим подразумевается переход локальная сеть – сеть Интернет, и все, за редким обоснованным исключением компьютеры сети, связываются с Интернет только через шлюз

Компоненты

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 необходима 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 приятном и удобном виде вывести данные с сервера администрирования, на их основе построить графики и диаграммы, 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.

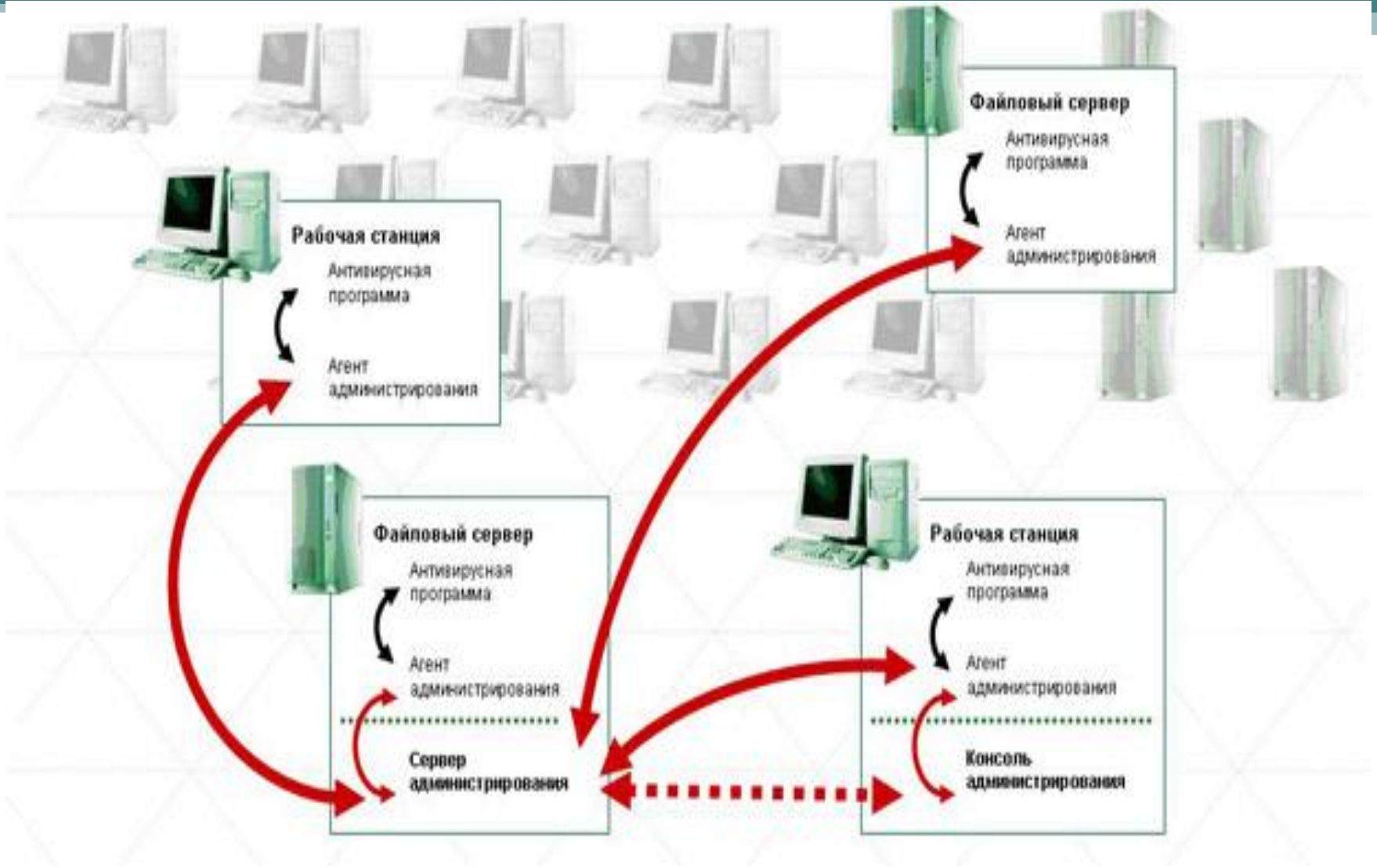


Схема взаимодействия компонентов централизованно управляемого комплекса для защиты рабочих станций и сетевых серверов

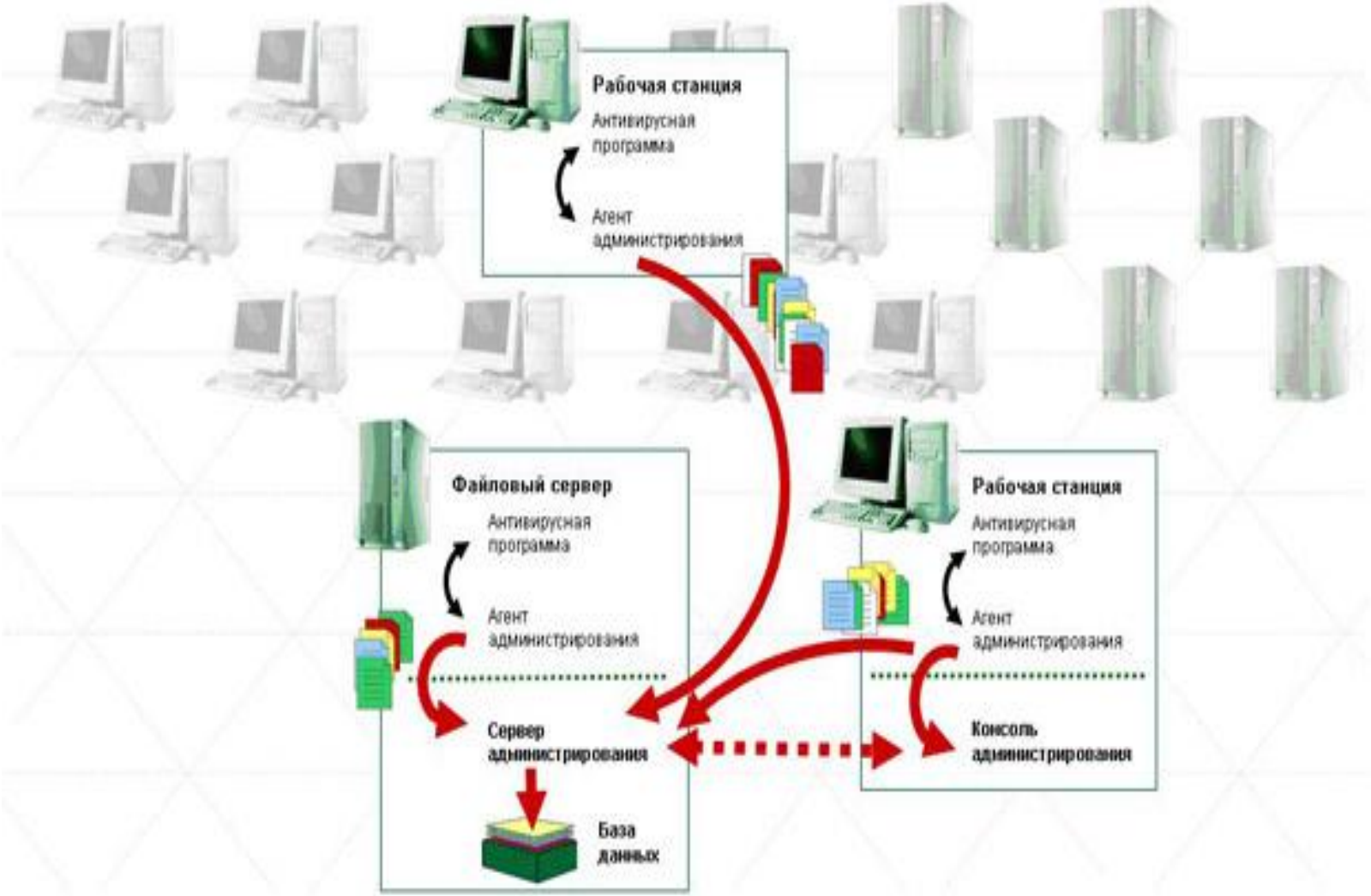


Схема сбора статистики в системе антивирусной защиты

- Приведенная схема реализована в большинстве популярных антивирусных комплексов, однако существуют программы, которые немного иначе распределяют функции среди своих компонентов. Однако общий алгоритм работы системы удаленного централизованного управления остается таким же.