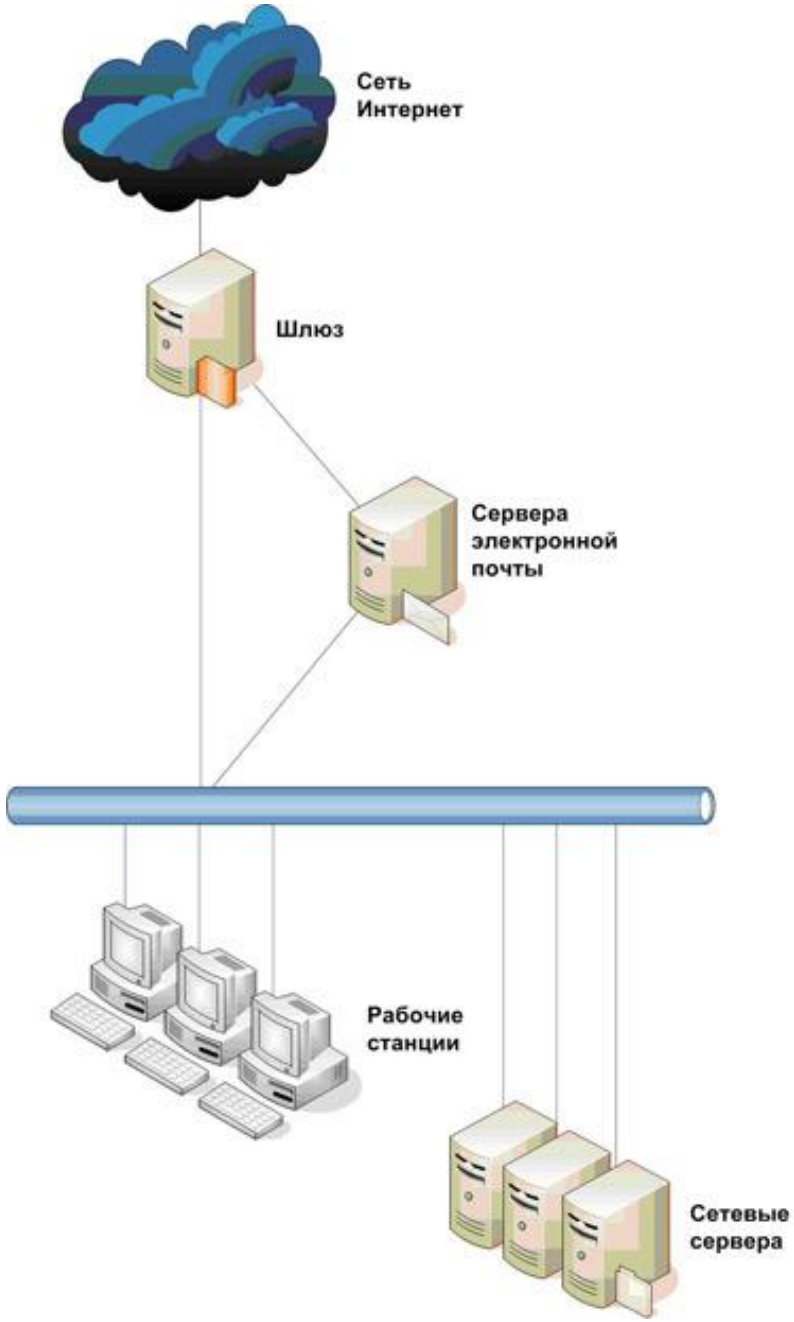
Тема занятия:

Построение антивирусной защиты корпоративной сети

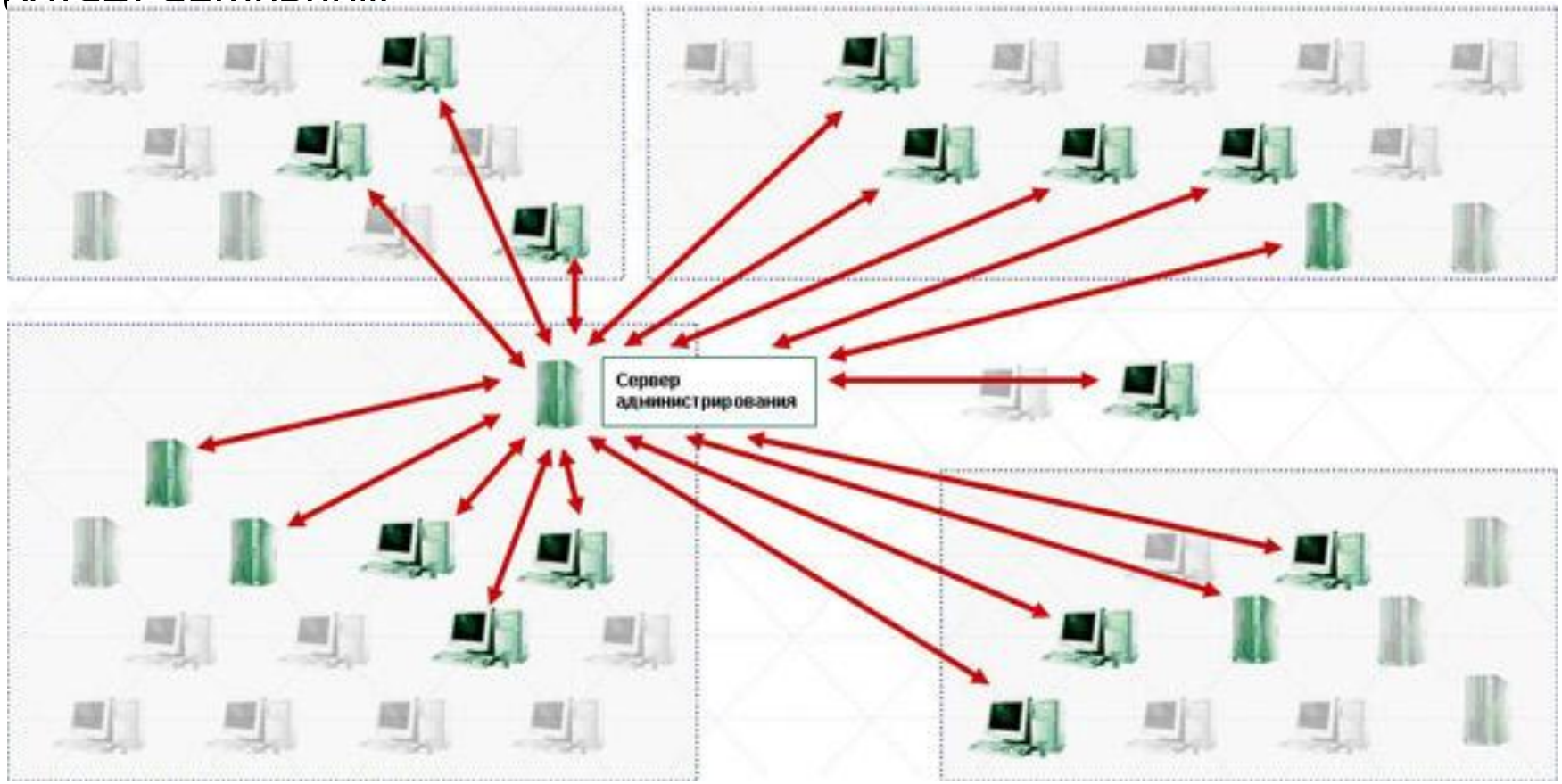
Цель: изучить методы и средства защиты корпоративной среды



Типовая локальная компьютерная сеть:

1. **Рабочие станции и сетевые сервера** - обмен файлами по сети и с помощью мобильных носителей
2. **Почтовые сервера** - прием и отправка электронных писем, иногда обмен файлами по сети и с помощью мобильных носителей
3. **Шлюз** - организация обмена файлов между компьютерами локальной сети и более глобальной сетью, например Интернет.

Существуют **системы удаленного централизованного управления антивирусной защитой,** которые позволяют администратору обслуживать все входящие в его ведение рабочие станции и сетевые сервера: удаленно настраивать политики антивирусной безопасности, запускать проверку объектов на наличие в них вирусов, включать или выключать постоянную защиту, централизованно обновлять антивирусные базы, 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 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 удобном виде вывести данные с сервера администрирования, на их основе построить графики и диаграммы, создать отчеты, произвести настройку клиентских

Основанием для подозрения на наличие вируса в системе могут служить:

- Внезапное и несанкционированное изменение настроек браузера
- Необычные всплывающие окна и другие сообщения
- Неожиданный несанкционированный дозвон в Интернет
- Самопроизвольное блокирование антивирусной программы
- Невозможность загрузки файлов с веб-сайтов антивирусных компаний
- Необоснованные на первый взгляд сбои в работе операционной системы или других программ
- Почтовые уведомления с заслуживающих доверие сайтов об отправке пользователем инфицированных сообщений

Для проверки работоспособности установленной антивирусной защиты существует специальный **тестовый вирус - Eicar**. Все ведущие антивирусные продукты его детектируют, при этом никаких действий он не совершает.

Для предотвращения проникновения в систему вредоносной программы необходимо соблюдать следующие правила:

- Вовремя устанавливать последние обновления и патчи используемого программного обеспечения, особенно - операционной системы семейства Microsoft Windows;
- Перед чтением данных с любого сменного носителя (flash-память и др.) обязательно проводить проверку на наличие на нем вирусов;
- Не загружать из Интернет файлы неизвестного происхождения, тем более - программы, и не устанавливать их. Особенно это касается не заслуживающих доверия сайтов;
- Не открывать электронные письма, полученные от незнакомых людей или имеющие подозрительную тему сообщения;
- Если на компьютере установлен антивирус - никогда не выключать постоянную проверку, поддерживать актуальность антивирусных баз, каждую неделю проводить тщательную проверку всего диска на наличие на нем вирусов;
- Использование брандмауэра, пусть даже встроенного в операционную систему, также крайне желательно;
- Самостоятельно даже не пытаться создавать вредоносные программы или сознательно участвовать в их распространении, поскольку в *Уголовном Кодексе* Российской Федерации есть ряд статей, предусматривающих наказание за такую деятельность, вплоть до лишения свободы на срок до пяти лет, а современные технологии позволяют достаточно быстро вычислить автора или распространителя.

В своей работе антивирус использует следующие технологии:

- Сигнатурный анализ
- Эвристический анализ

Сигнатурный анализ требует наличия самых последних антивирусных баз - списка *сигнатур вирусов*.

Эвристический анализ — метод обнаружения вредоносных программ, при котором антивирусная программа контролирует все действия, выполняемые проверяемой программой. В ходе эвристического анализа отслеживаются потенциально опасные действия, характерные для вирусов и вредоносных программ других типов.

Для обеспечения эффективной антивирусной защиты используются два основные режима работы антивирусного программного обеспечения:

- Проверка в режиме реального времени или постоянная защита;
- Проверка по требованию.

В первом случае обеспечивается защита от заражения системы, во втором - от проникновения вредоносных программ.

Литература для самостоятельного изучения:

1. Антивирусная защита компьютерных систем