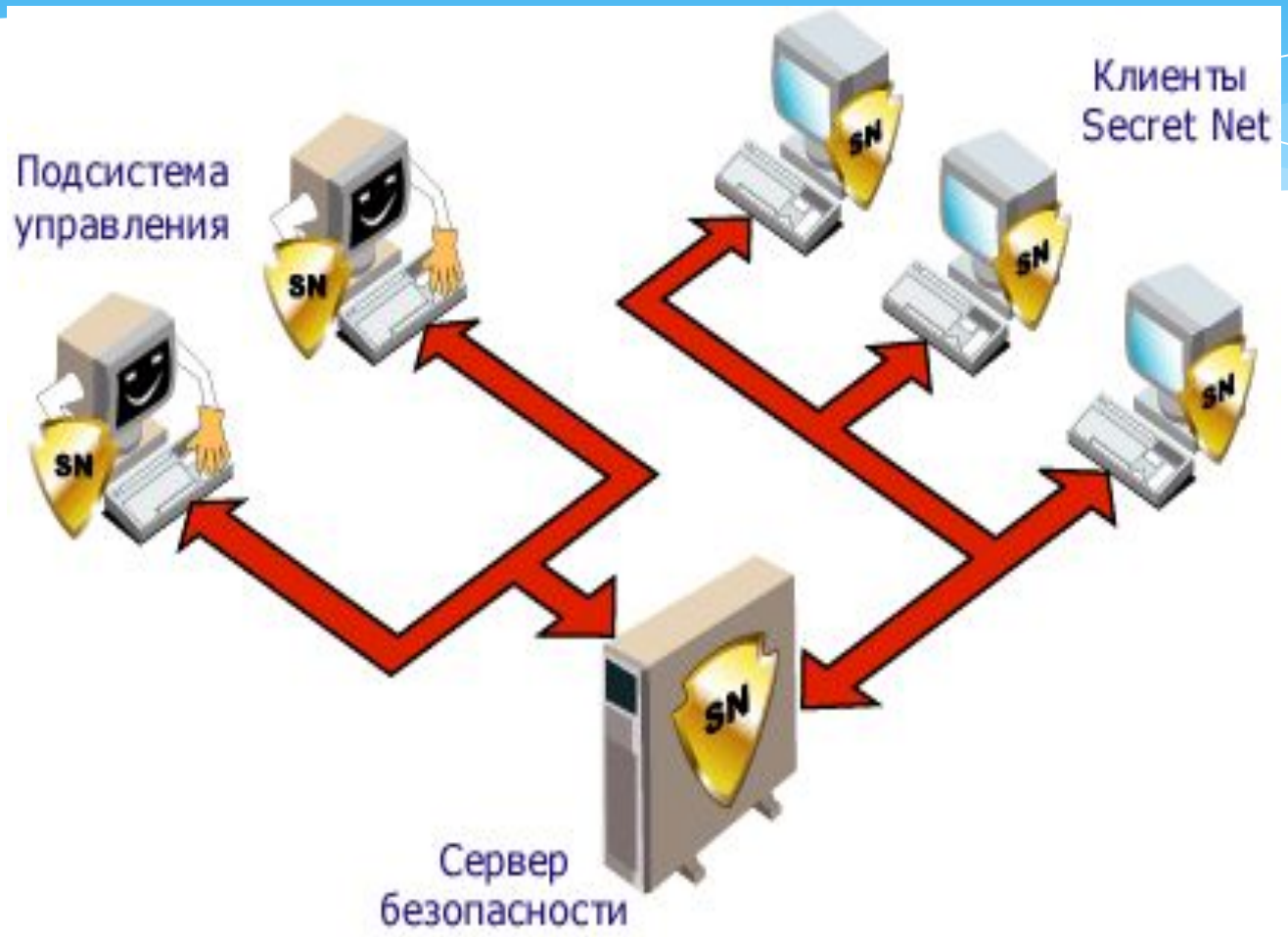
Информационная безопасность

Аппаратные средства защиты информации

* Аппаратные средства защиты информации – это различные технические устройства , системы и сооружения , предназначенные для защиты информации от разглашения , утечки и несанкционированного доступа.


WWW
WWW
WWW
WWW


Клиенты
Secret Net
Подсистема
управления
SN
SN
SN
SN
SN
SN
Сервер
безопасности

Программные средства защиты информации

* SFT Level I. Первый уровень предусматривает, в частности, создание дополнительных копий FAT и Directory Entries Tables, немедленную верификацию каждого в'новь записанного на файловый сервер блока данных, а также резервирование на каждом жестком диске около 2% от объема диска. При обнаружении сбоя данные перенаправляются в зарезервированную область диска, а сбойный блок помечается как «плохой» и в дальнейшем не используется.

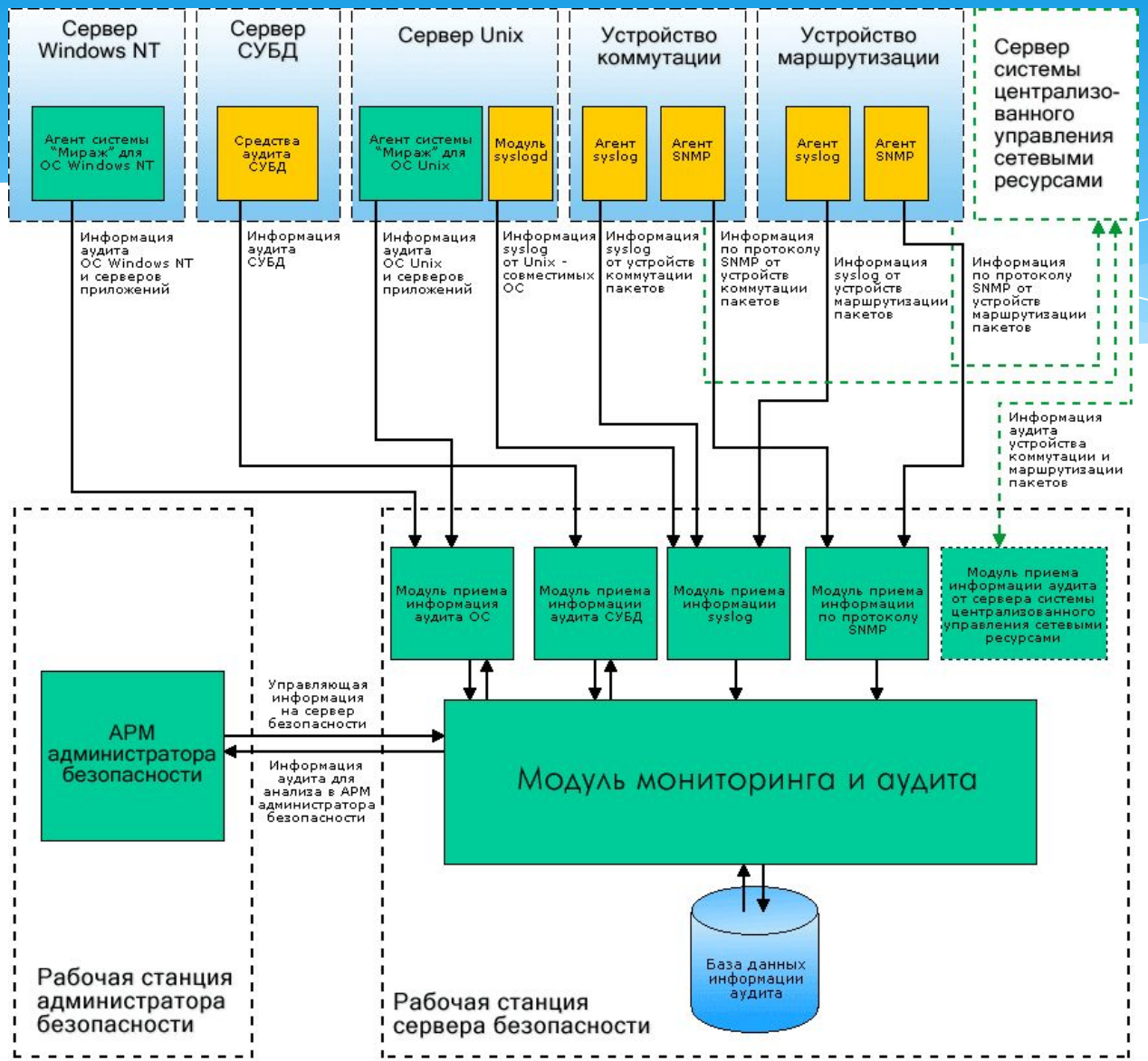
* SFT Level II содержит дополнительно возможности создания «зеркальных» дисков, а также дублирования дисковых контроллеров, источников питания и интерфейсных кабелей.

* SFT Level III позволяет использовать в локальной сети дублированные серверы, один из которых является «главным», а второй, содержащий копию всей информации, вступает в работу в случае выхода «главного» сервера из строя.

Специализированные программные средства защиты информации

* Firewalls - брандмауэры (дословно firewall — огненная стена). Между локальной и глобальной сетями создаются специальные промежуточные сервера, которые инспектируют и фильтруют весь проходящий через них трафик сетевого/ транспортного уровней. Это позволяет резко снизить угрозу несанкционированного доступа извне в корпоративные сети, но не устраняет эту опасность совсем. Более защищенная разновидность метода - это способ маскарада (masquerading), когда весь исходящий из локальной сети трафик посылается от имени firewall-сервера, делая локальную сеть практически невидимой.

* Proxy-servers (proxy - доверенность, доверенное лицо). Весь трафик сетевого/транспортного уровней между локальной и глобальной сетями запрещается полностью — попросту отсутствует маршрутизация как таковая, а обращения из локальной сети в глобальную происходят через специальные серверы-посредники. Очевидно, что при этом методе обращения из глобальной сети в локальную становятся невозможными в принципе. Очевидно также, что этот метод не дает достаточной защиты против атак на более высоких уровнях - например, на уровне приложения (вирусы, код Java и JavaScript).


Сервер Windows NT
Агент системы "Мираж" для ОС Windows NT
Сервер СУБД
Средства аудита СУБД
Сервер Unix
Агент системы "Мираж" для ОС Unix
Модуль syslogd
Устройство коммутации
Агент syslog
Агент SNMP
Устройство маршрутизации
Агент syslog
Агент SNMP
Сервер системы централизо-ванного управления сетевыми ресурсами
Информация аудита ОС Windows NT и серверов приложений
Информация аудита СУБД
Информация аудита ОС Unix и серверов приложений
Информация syslog от Unix - совместимых ОС
Информация syslog от устройств коммутации пакетов
Информация по протоколу SNMP от устройств коммутации пакетов
Информация syslog от устройств маршрутизации пакетов
Информация по протоколу SNMP от устройств маршрутизации пакетов
Информация аудита устройства коммутации и маршрутизации пакетов
Модуль приема информация аудита ОС
Модуль приема информации аудита СУБД
Модуль приема информации syslog
Модуль приема информации по протоколу SNMP
Модуль приема информации аудита от сервера системы централизованного управления сетевыми ресурсами
АРМ администратора безопасности
Управляющая информация на сервер безопасности
Информация аудита для анализа в АРМ администратора безопасности
Модуль мониторинга и аудита
База данных информации аудита
Рабочая станция администратора безопасности
Рабочая станция сервера безопасности