Лекция 11. Защита информации в Интернет

Глобальная сеть Internet

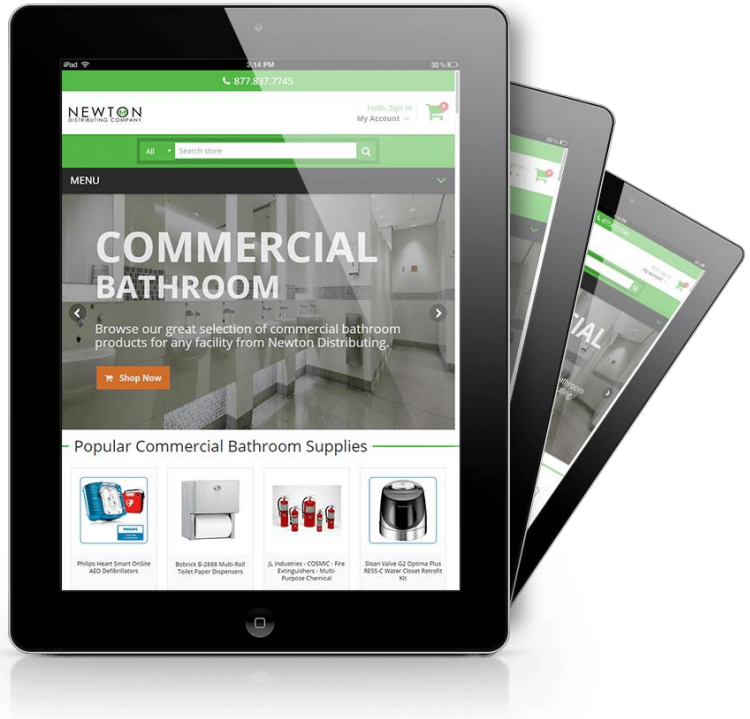
вторгнуться во внутреннюю сеть предприятия и получить несанкционированный доступ к конфиденциальной информации;

незаконно скопировать важную и ценную для предприятия

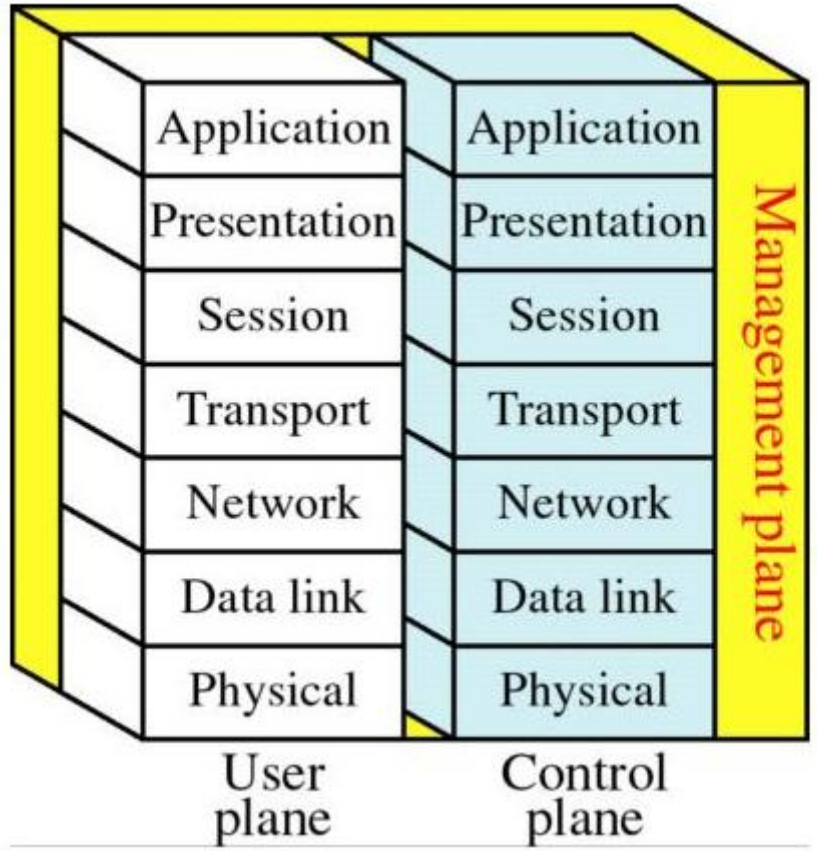
- информацию;

получить пароли, адреса серверов, а подчас и их содержимое;

входить в информационную систему предприятия под именем зарегистрированного пользователя и т.д.



Tranmission Control Protocol/ Internet Protocol – TCP/IP



Simple Mail Transfer Protocol - SMTP

Send-mail

File Transfer Protocol - FTP

Domain Name System- DNS

TELNET

Word Wide Web - WWW

Политика сетевой безопасности

политику доступа к сетевым сервисам;

политику реализации межсетевых экранов.

Политика доступа к сетевым сервисам

Запретить доступ из Интернет во внутреннюю сеть, но разрешить доступ из внутренней сети в Интернет;

Разрешить ограниченный доступ во внутреннюю сеть из Интернет, обеспечивая работу только отдельных «авторизированных» систем

требования к фильтрации на сетевом уровне;

требования к фильтрации на прикладном уровне;

требования по настройке правил фильтрации и администрированию;

требования к средствам сетевой аутентификации;

требования по внедрению журналов и учету.

Стандарты и способы защиты информации в Интернет

Защита Web - приложений: S – HTTP и SSL

Стандарт	Функция	Применение
Secure HTTP (S-HTTP)	Защита транзакций в **Web**	Браузеры, **Web**-серверы, приложения для Интернета
Secure Sockets Layer (SSL)	Защита пакетов данных на сетевом уровне	Браузеры, **Web**-серверы, приложения в Интернете.
Secure MIME (S/MIME)	Защита вложений в электронные послания на различных платформах	Почтовые программы с поддержкой шифрования и цифровой подписи RSA
Secure Wide-Area Networks (S/WAN)	Шифрование одно-ранговых соединений между Брандмауэрами и маршрутизаторами	Виртуальные частные сети
Secure Electronic Transaction (SET)	Защита транзакций с кредитными картами	Смарт -карты, серверы транзакций, электронная коммерция.

Защита электронной почты: PEM, S/MIME и PGP

Права собственности и законности информации в Internet

Метод открытого ключа (Public Key Encryption),

Pretty Good Privacy (высокая степень секретности)

- доступной;
- удобной;
- криптографически надёжной;
- законной;
- заслуживающей доверия;
- широко распространённой.

Система криптографической защиты информации от НСД КРИПТОН – ВЕТО.

· абонентского пункта;

· центра коммутации пакетов;

· центра выработки ключей.

· обеспечение секретности информации в случае кражи «винчестера» или ПК;

· обеспечение защиты от несанкционированного включения компьютера;

· разграничение полномочий пользователя по доступу к ресурсам компьютера;

· проверка целостности программы в момент ее запуска на выполнение;

· ведение системного журнала, регистрирующего события, возникающие в системе;

· обеспечение «прозрачного» шифрования информации при обращении к защищенному диску;

· обнаружение искажений, вызванных вирусами, ошибками пользователей, техническими сбоями и действиями злоумышленника.

Комплекс КРИПТОН-ЗАМОК для ограничения доступа к компьютеру

· ограничивает доступ пользователей к компьютеру путем их идентификации и аутентификации;

· разделяет доступ пользователей к ресурсам компьютера в соответствии с их полномочиями;

· контролирует целостность ядра комплекса, программ операционной среды, прикладных программ и областей памяти;

· регистрирует события в защищенном электронном журнале;

· передает управление и параметры пользователя программному обеспечению (RUN - файлам), указанному администратором.

CRLOCK.EXE

· в компьютер может войти только санкционированный пользователь;

· загружается достоверное ядро комплекса;

· загружается достоверная ОС;

· проверяется целостность прикладного ПО, указанного администратором;

· производится запуск программ, указанных администратором.

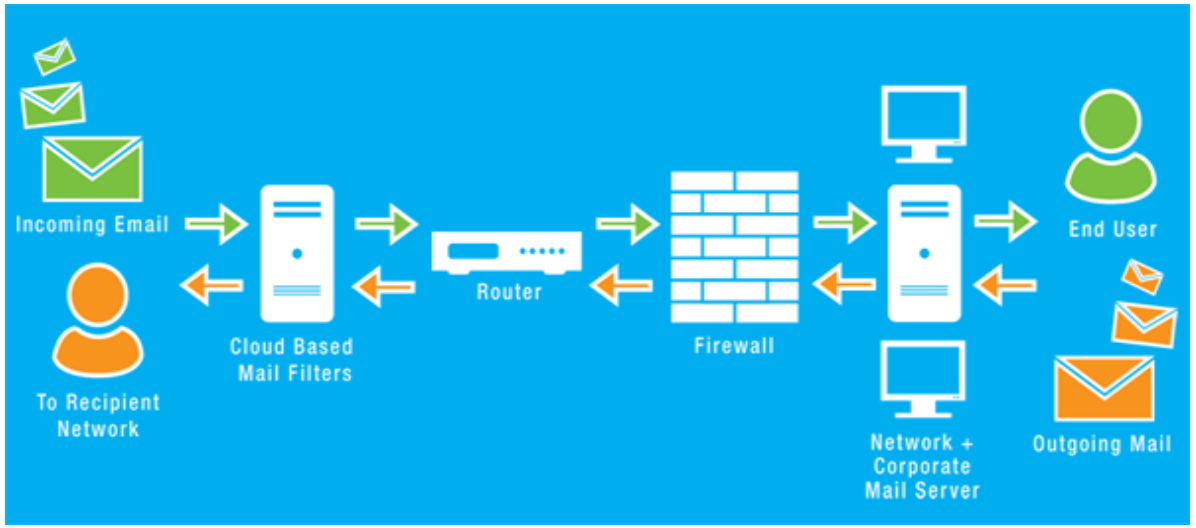
Система защиты конфиденциальной информации Secret Disk

абонентское шифрование (АШ);

электронная цифровая подпись (ЭЦП);

пакетное шифрование (ПШ);

криптографическая аутентификация абонентов.



Программа электронной цифровой подписи Crypton Sign

Программа Crypton Sign предназначена для формирования и проверки электронной цифровой подписи электронных документов, которая обеспечивает установление авторства электронных документов и проверку целостности электронных документов.

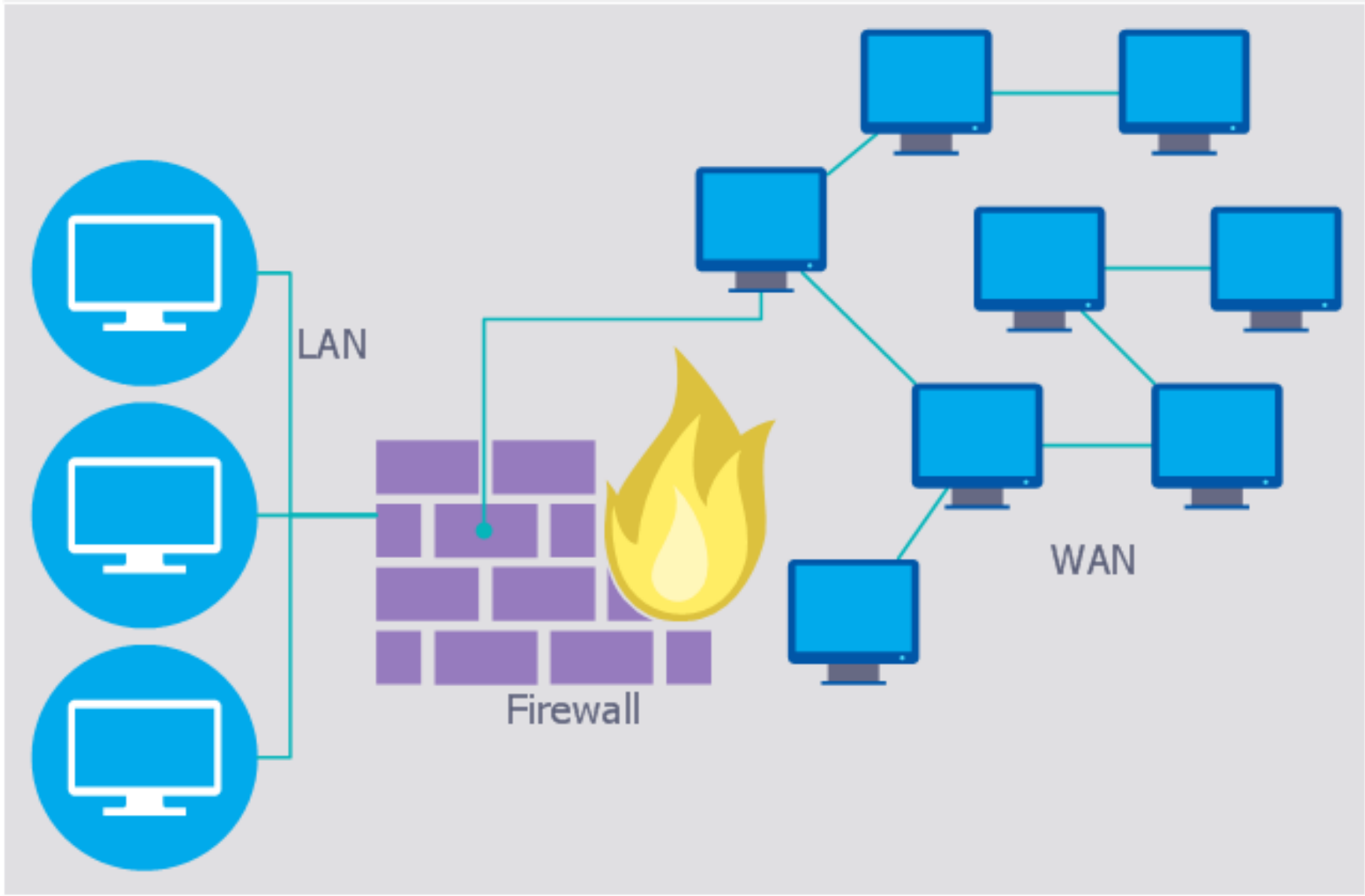
Генерация случайного кода для создания ключей выполняется аппаратно с одного из УКЗД серии КРИПТОН. Если УКЗД в компьютере нет, случайный код можно получить программно с помощью программы Crypton LITE или генератора случайных чисел.

Электронная цифровая подпись (ЭЦП) представляет собой последовательность байтов, помещаемую в конец подписываемого документа или в отдельный файл. **ЭЦП** формируется на основании содержимого документа, секретного ключа и пароля лица, подписывающего документ. Для каждого секретного ключа создается открытый ключ для проверки подписи.

В качестве подписываемого электронного документа в программе может использоваться любой файл.

- Для управления программой **Crypton Sign** пользователю необходим интерфейс, похожий на интерфейс Norton Commander. Основное меню программы **Crypton Sign** разделено на две части (панели). В левой части меню расположены наименования команд, выполняемых программой, в правой части – перечень файлов и раздел, в котором находятся эти файлы. Для выбора команд и файлов используется маркер.
- Схема создания и проверки **ЭЦП** с помощью программы **Crypton Sign** показана на рис.6.2. Для формирования и последующей проверки подписи необходимо создать два ключа-подписи: секретный и открытый. Ключи представляют собой обычные файлы на дискете или последовательность байтов на электронной карточке.

Брандмауэрные системы защиты



Межсетевой экран (МЭ)

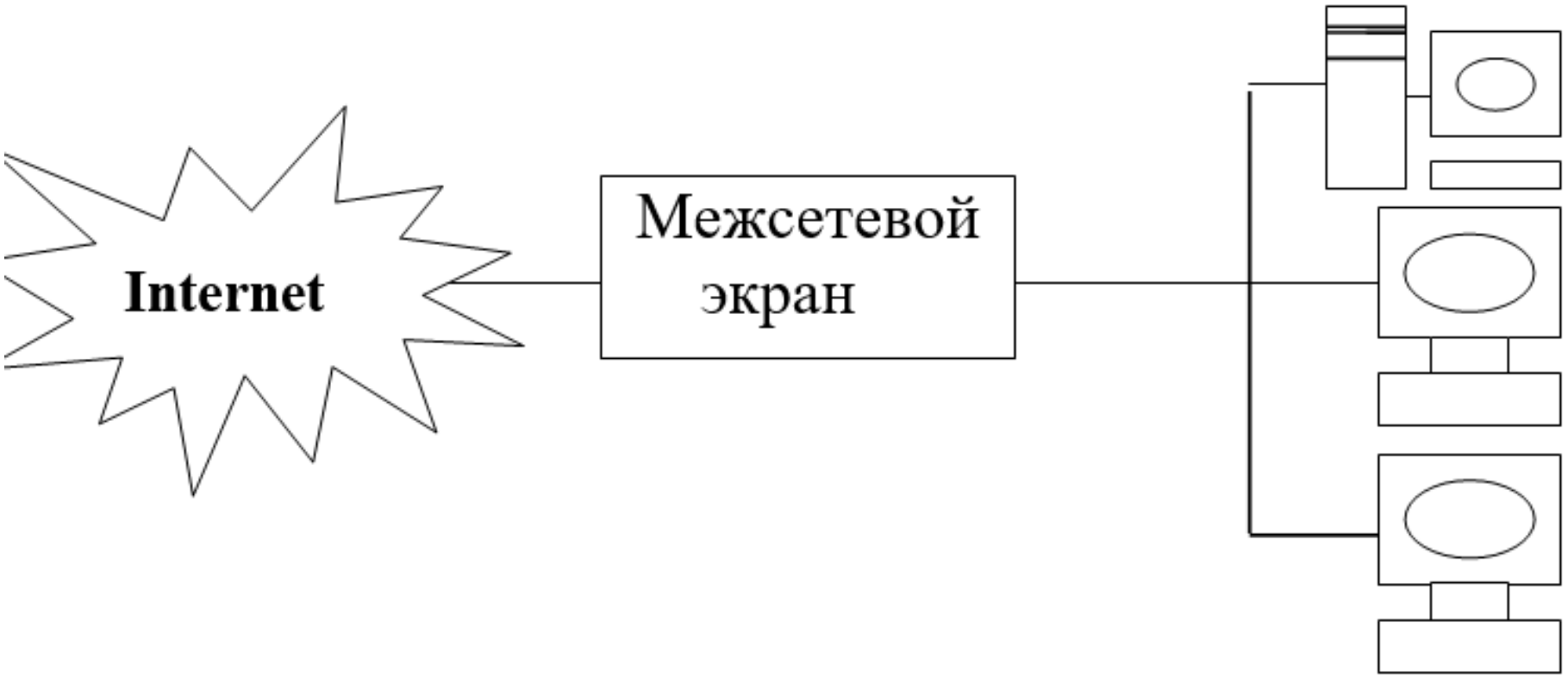


Схема установления межсетевого экрана.

Основные компоненты межсетевых экранов

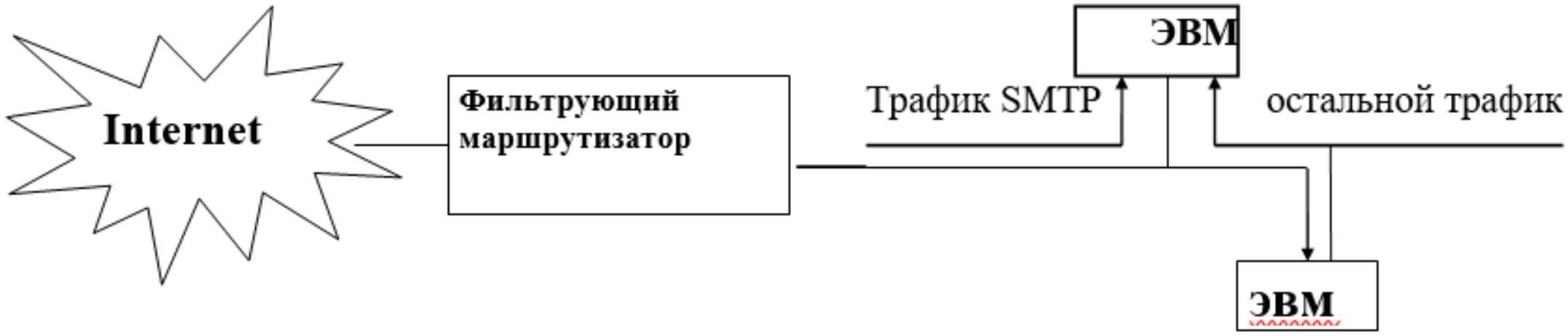


Схема фильтрации трафика SMTP и TELNET

К положительным качествам фильтрующих маршрутизаторов следует отнести:

- сравнительно невысокую стоимость;
- гибкость в определение правил фильтрации;
- небольшую задержку при прохождении пакетов.

Недостатками фильтрующих маршрутизаторов являются

- внутренняя сеть видна (маршрутизируется) из сети Internet;
- правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологии TCP и UDP;
- работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными
- атакующая система выдает себя за другую, используя и IP-адрес.

Шлюзы прикладного уровня имеют ряд серьезных преимуществ по сравнению с обычным режимом, при котором прикладной трафик пропускается непосредственно к внутренним хост-компьютерам:

- невидимость структуры защищаемой сети из глобальной сети Internet;
- надежная регистрация;
- оптимальное соотношение между ценой и эффективностью;
- простые правила фильтрации;
- возможность организации большого числа проверок.

К недостаткам шлюзов прикладного уровня относятся:

- более низкая производительность по сравнению с фильтрующими маршрутизаторами;
- более высокая стоимость по сравнению с фильтрующими маршрутизаторами.

канальные посредники

полномочные сервера

шлюз прикладного уровня