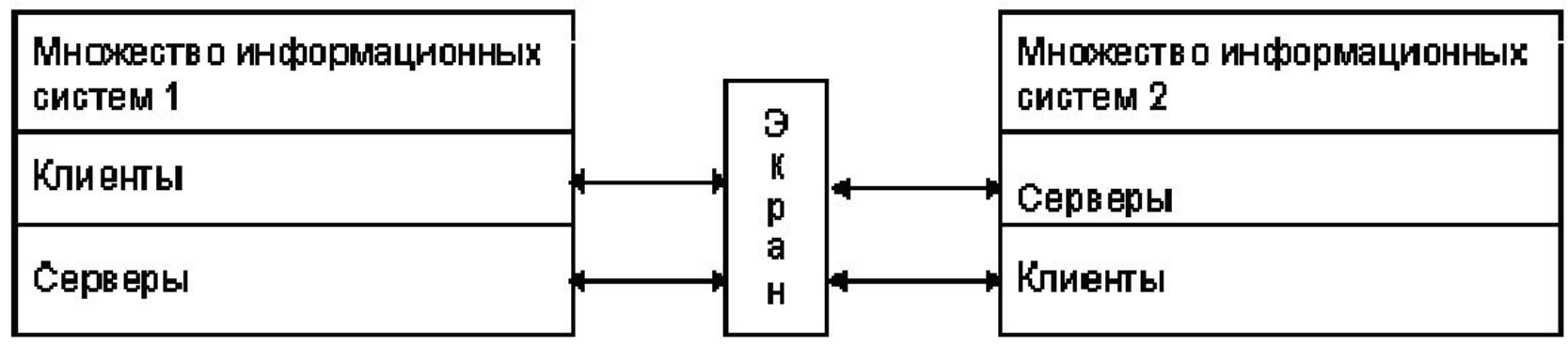
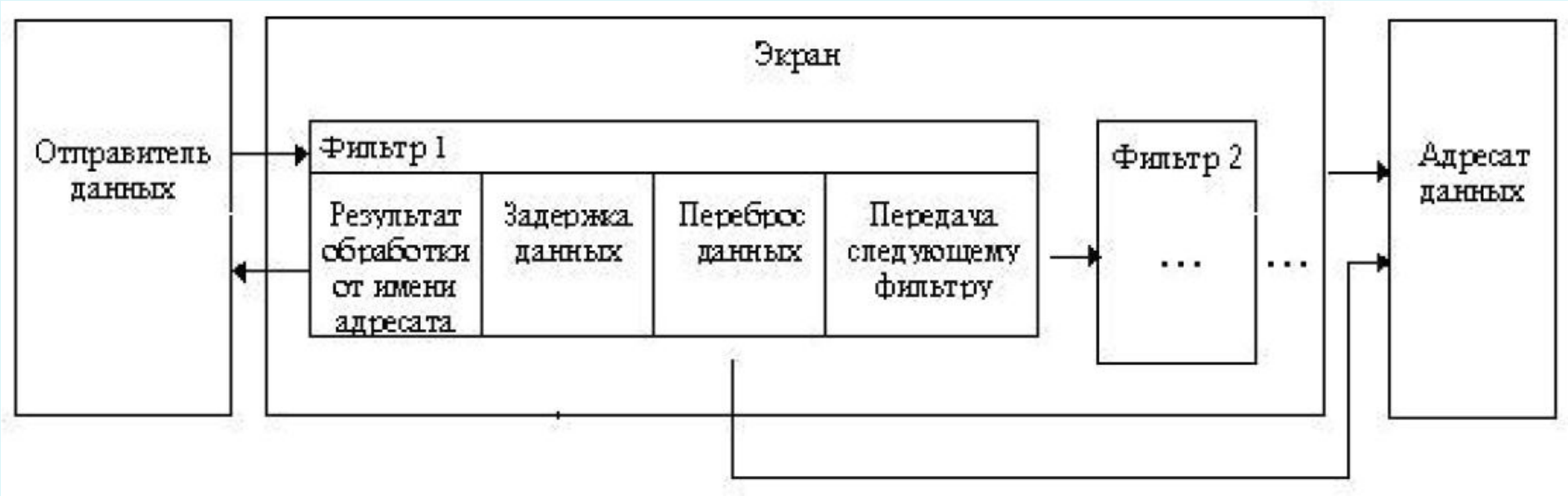
МЕЖСЕТЕВЫЕ ЭКРАНЫ

Межсетевой экран (*англ. -firewall; нем. -Brandmauer*) – средство разграничения доступа клиентов из одного множества систем к информации, хранящейся на серверах в другом множестве.



МЭ можно представить как **набор фильтров**, анализирующих проходящую через них информацию и принимающих решение: пропустить информацию или её заблокировать.



Обычно экранирующие системы делаются несимметричными. Для экранов определяются понятия “внутри” и “снаружи”.

Современные требования к межсетевым экранам

1. Обеспечение безопасности внутренней (защищаемой) сети и полный контроль над внешними подключениями и сеансами связи.

2. Мощные и гибкие средства управления.

3. МЭ должен работать незаметно для пользователей.

4. Процессор межсетевого экрана должен быть быстродействующим.

5. Система обеспечения безопасности должна быть сама надежно защищена от любых несанкционированных воздействий.

6. Возможность централизованно обеспечивать проведение единой политики безопасности для удаленных филиалов.

7. Межсетевой экран должен иметь средства авторизации доступа пользователей через внешние подключения.

Классификация межсетевых экранов

По способу реализации:

- программные,
- аппаратно-программные.

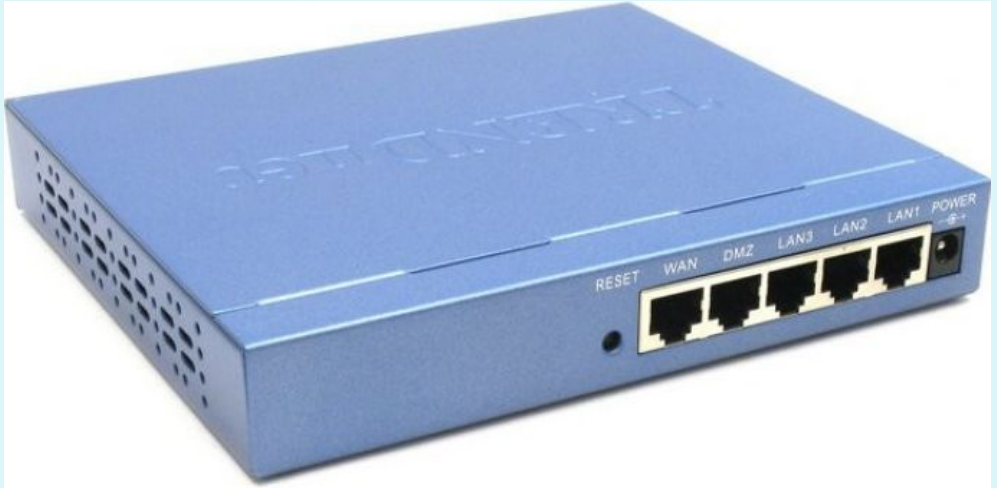
По типу защищаемого объекта:

- сегментные МЭ, устанавливаемые на границе двух или более сетей,
- встраиваемые МЭ, функционирующие на одной платформе с защищаемыми серверами,
- персональные МЭ.

Классы МЭ по принципу действия:

- **Фильтрующие маршрутизаторы.**

Фильтрующий маршрутизатор представляет собой маршрутизатор или работающую на сервере программу, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты. Фильтрация пакетов осуществляется на основе информации, содержащейся в TCP- и IP-заголовках пакетов.



- **Шлюзы сеансового уровня**.

Представляет собой транслятор TCP-соединения. Шлюз принимает запрос авторизованного клиента на конкретные услуги и после проверки допустимости запрошенного сеанса устанавливает соединение с местом назначения (внешним хостом). Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, не проводя никакой фильтрации.

- **Шлюзы уровня приложений.**

Представляет собой хост, на котором работает proxy-служба. Proxy-служба – это прикладные программы для фильтрации соединений с такими сервисами, как Telnet и FTP. Взаимодействие с внешним миром реализуется через небольшое число уполномоченных приложений, полностью контролирующих весь входящий и исходящий трафик.