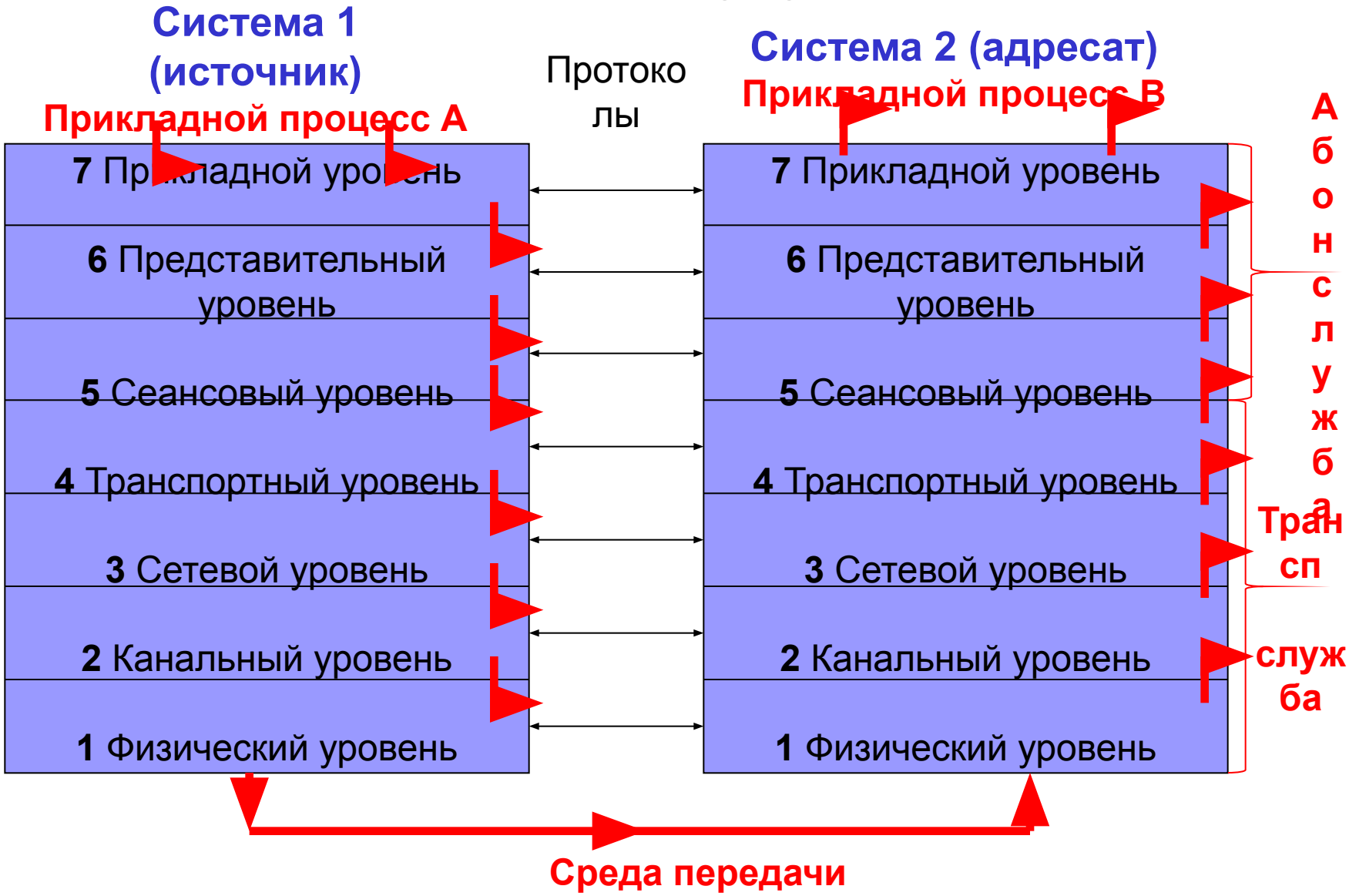
Обеспечение безопасности в компьютерных сетях

Основные принципы, технологии, протоколы

Эталонная модель взаимодействия открытых систем

OSI – обобщенная логическая структура вычислит. сети



Основные угрозы в открытых сетевых системах

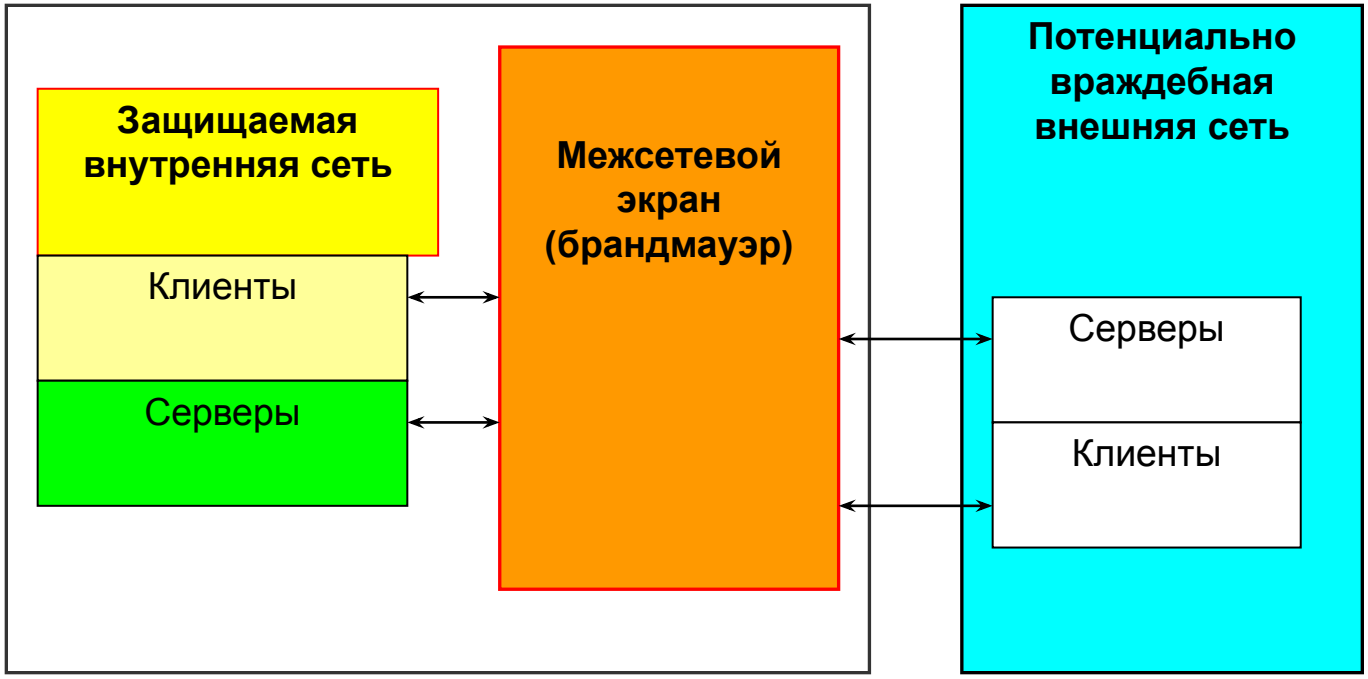
- угрозы неправомерного вторжения во внутреннюю сеть из внешней;
- угрозы несанкционированного доступа во внешнюю сеть из внутренней.

Ограничение разрешенного доступа во внешнюю сеть

- для предотвращения утечки конфиденциальных данных;
- при запрете доступа, например, в учебных заведениях, к информации нецензурной и нежелательной направленности;
- в случае запрета служебного доступа к развлекательным компьютерным ресурсам в рабочее время.

Функции межсетевого экранирования

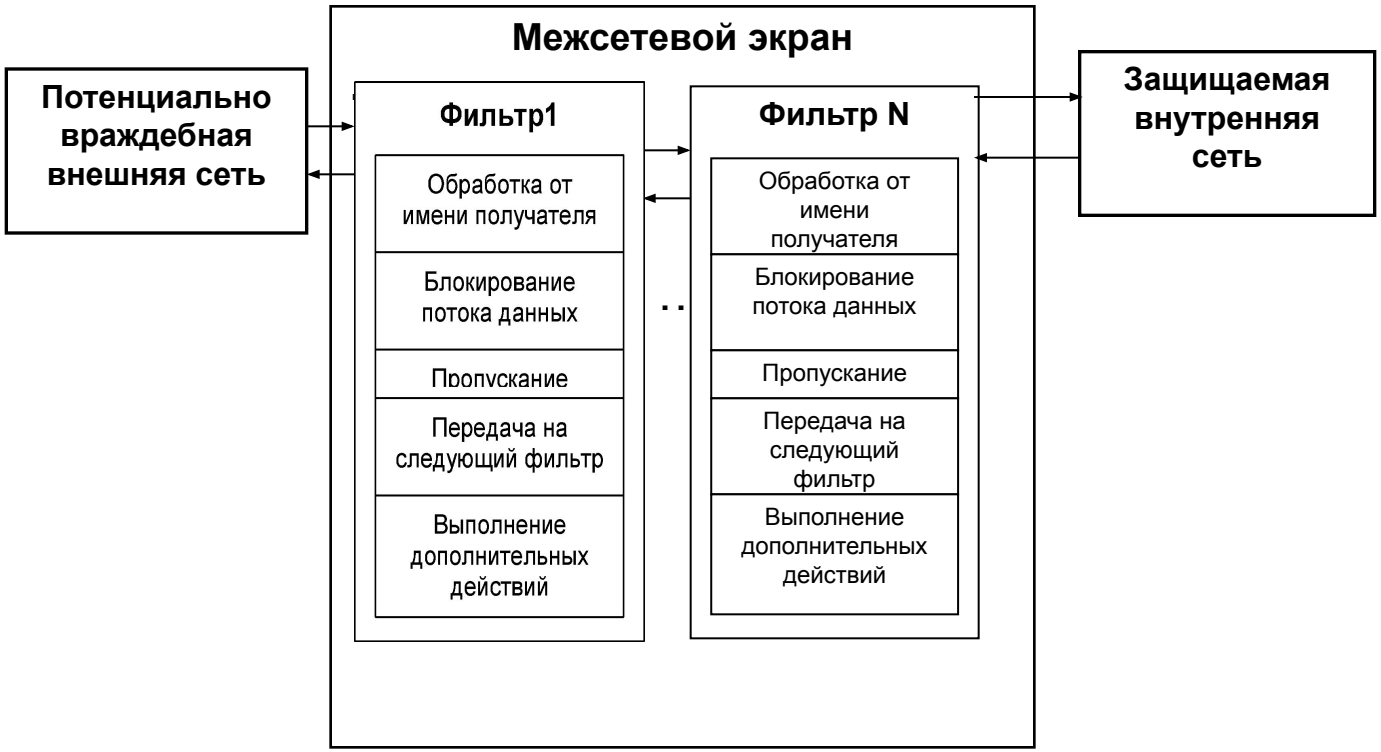
Схема подключения межсетевого экрана



Основные анализируемые элементы

- *Информация о соединениях* — информация от всех семи уровней модели OSI в пакете.
- *История соединений* — информация, полученная от предыдущих соединений. Например, исходящая команда PORT сессии FTP должна быть сохранена для того, чтобы в дальнейшем можно было проверить входящее соединение FTP data.
- *Состояние уровня приложения* — информация о состоянии, полученная из других приложений. Например, аутентифицированному до настоящего момента пользователю можно предоставить доступ через брандмауэр только для авторизованных видов сервиса.
- *Агрегирующие элементы* — вычисления разнообразных выражений, основанных на всех вышеперечисленных факторах.

Структура межсетевого экрана



Стадии фильтрации

1. Анализ информации по заданным в интерпретируемых правилах критериям, например, по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена.
2. Принятие на основе интерпретируемых правил одного из следующих решений:

- не пропустить данные;
- обработать данные от имени получателя и возвратить результат отправителю;
- передать данные на следующий фильтр для продолжения анализа;
- пропустить данные, игнорируя следующие фильтры.

Условия фильтрации

- разрешение или запрещение дальнейшей передачи данных;
- выполнение дополнительных защитных функций

Критерии анализа информационного потока

- служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;
- непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие компьютерных вирусов;
- внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и другие.

Основные функции межсетевого экрана

1. идентификация и аутентификация пользователей;
2. проверка подлинности передаваемых данных;
3. разграничение доступа к ресурсам внутренней сети;
4. разграничение доступа к ресурсам внешней сети;
5. фильтрация и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
6. трансляция внутренних сетевых адресов для исходящих пакетов сообщений;
7. регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерацию отчетов;
8. кэширование данных, запрашиваемых из внешней сети;

Типы межсетевых экранов

- *экранирующий маршрутизатор*, работающий на третьем, сетевом уровне эталонной моделиOSI;
- *экранирующий транспорт* (шлюз сеансового уровня), работающий на пятом, сеансовом уровне модели OSI;
- *экранирующий шлюз* (шлюз прикладного уровня), работающий на седьмом, прикладном уровне модели OSI.