МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ   
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ   
«ВЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Институт математики и информационных систем

ФАКУЛЬТЕТ КОМПЬЮТЕРНЫХ И ФИЗИКО-МАТЕМАТИЧЕСКИХ НАУК

КАФЕДРА ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ

**Межсетевое экранирование. определения. Постановка задачи. Классификация межсетевых экранов.**

Доклад

по дисциплине «Информационная безопасность»

Выполнил студент группы ФИб-4302-51-00   / Савин Д.А. /

Киров 2022

**Основные понятия**

***Экран*** – это средство *разграничения доступа* клиентов из одного множества к серверам из другого множества. *Экран* осуществляет свои функции, контролируя все информационные потоки между двумя множествами систем (рис.1). Контроль потоков состоит в их *фильтрации*, возможно, с выполнением некоторых преобразований.

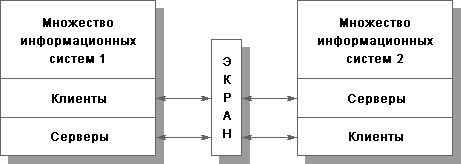


Рис.1 - Экран как средство разграничения доступа.

На следующем уровне детализации *экран* (полупроницаемую мембрану) удобно представлять как последовательность *фильтров*. Каждый из *фильтров*, проанализировав данные, может задержать (не пропустить) их, а может и сразу "перебросить" за *экран*. Кроме того, допускается преобразование данных, передача порции данных на следующий *фильтр* для продолжения анализа или обработка данных от имени адресата и возврат результата отправителю (рис.2).

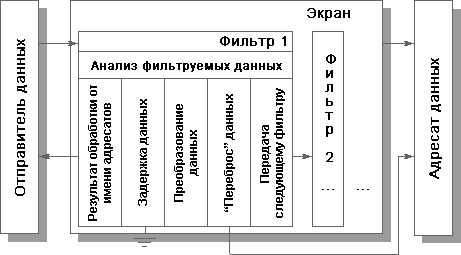


Рис.2 - Экран как последовательность фильтров

*Межсетевой экран* – идеальное место для встраивания средств активного аудита. *МЭ* способен реализовать сколь угодно мощную реакцию на подозрительную активность, вплоть до разрыва связи с внешней средой.

На *межсетевой экран* целесообразно возложить идентификацию/аутентификацию внешних пользователей, нуждающихся в доступе к корпоративным ресурсам (с поддержкой концепции единого входа в сеть).

**Принципы работы межсетевых экранов**

Существует два основных способа создания наборов правил межсетевого экрана: ''включающий'' и ''исключающий''. Исключающий межсетевой экран позволяет прохождение всего трафика, за исключением трафика, соответствующего набору правил. Включающий межсетевой экран действует прямо противоположным образом. Он пропускает только трафик, соответствующий правилам и блокирует все остальное.

Включающие межсетевые экраны обычно более безопасны, чем исключающие, поскольку они существенно уменьшают риск пропуска межсетевым экраном нежелательного трафика.

Безопасность может быть дополнительно повышена с использованием ''межсетевого экрана с сохранением состояния''. Такой межсетевой экран сохраняет информацию об открытых соединениях и разрешает только трафик через открытые соединения или открытие новых соединений. Недостаток межсетевого экрана с сохранением состояния в том, что он может быть уязвим для атак DoS (Denial of Service, отказ в обслуживании), если множество новых соединений открывается очень быстро. Большинство межсетевых экранов позволяют комбинировать поведение с сохранением состояния и без сохранения состояния, что оптимально для реальных применений.

#### Классификация межсетевых экранов

При рассмотрении любого вопроса, касающегося сетевых технологий, основой служит семиуровневая эталонная модель ISO/OSI. *Межсетевые экраны* также целесообразно классифицировать по уровню *фильтрации:*

* канальному,
* сетевому,
* транспортному,
* прикладному.

Соответственно, можно говорить об:

* **экранирующих концентраторах** (мостах, коммутаторах) (уровень 2),
* **маршрутизаторах** (уровень 3),
* о транспортном *экранировании* (уровень 4)
* о прикладных *экранах* (уровень 7).

Существуют также комплексные *экраны*, анализирующие информацию на нескольких уровнях. Таким образом, МЭ можно разделить на три типа:

* пакетные фильтры (packet filter)
* сервера прикладного уровня (application gateways)
* сервера уровня соединения (circuit gateways)

*Фильтрация* информационных потоков осуществляется *межсетевыми экранами* на основе **набора правил**, являющихся выражением сетевых аспектов политики безопасности организации. В этих правилах, помимо информации, содержащейся в фильтруемых потоках, могут фигурировать данные, полученные из окружения, например, текущее время, количество активных соединений, **порт**, через который поступил сетевой запрос, и т.д. Таким образом, в *межсетевых экранах* используется мощный логический подход к *разграничению доступа*.

Возможности *межсетевого экрана* непосредственно определяются тем, какая информация может использоваться в правилах *фильтрации* и какова может быть мощность наборов правил. Вообще говоря, чем выше уровень в модели ISO/OSI, на котором функционирует *МЭ*, тем более содержательная информация ему доступна и, следовательно, тем тоньше и надежнее он может быть сконфигурирован.