

ПРОЕКТИРОВАНИЕ ПОЛИТИКИ БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ СЕТИ ПРЕДПРИЯТИЯ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Семак А.Д.

Селезнев И.Л. – к.т.н., доцент

Обеспечение комплексной безопасности является необходимым условием функционирования любой компании. Эта «комплексность» заключается, прежде всего, в продуманности, сбалансированности защиты, разработке четких организационно-технических мер и обеспечении контроля над их исполнением.

Значительное внимание в политике безопасности уделяется вопросам обеспечения безопасности информации при ее обработке в автоматизированных системах: автономно работающих компьютерах и локальных сетях. Необходимо установить, как должны быть защищены серверы, маршрутизаторы и другие устройства сети, порядок использования сменных носителей информации, их маркировки, хранения, порядок внесения изменений в программное обеспечение.

Важнейшим устройством, обеспечивающим безопасность корпоративной сети предприятия, является межсетевой экран. Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Существует два принципа обработки поступающего трафика. Первый принцип гласит: «что явно не запрещено, то разрешено». В данном случае, если межсетевой экран получил пакет, не подпадающий ни под одно правило, то он передается далее. Противоположный принцип – «что явно не разрешено, то запрещено» – гарантирует гораздо большую защищенность, так как он запрещает весь трафик, который явно не разрешен правилами.

В большинстве случаев поддерживаемый уровень сетевой модели OSI является основной характеристикой при их классификации (рисунок 1). Учитывая данную модель, различают следующие типы межсетевых экранов:

- 1) управляемые коммутаторы;
- 2) пакетные фильтры;
- 3) шлюзы сеансового уровня;
- 4) посредники прикладного уровня;
- 5) инспекторы состояния.

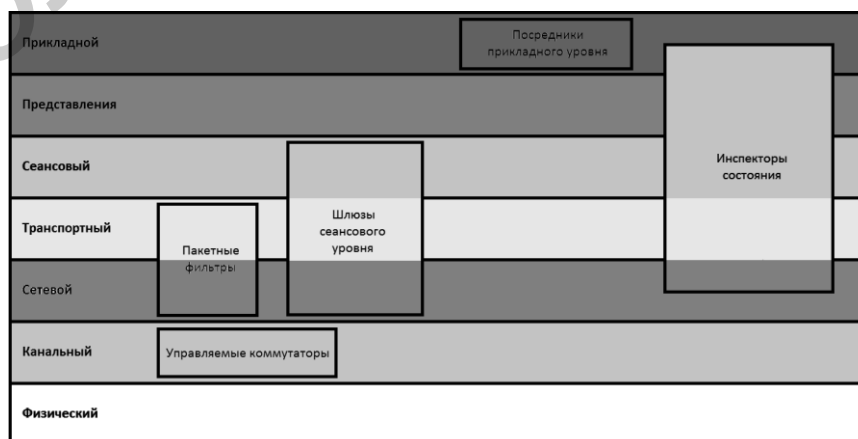


Рисунок 1 – Схематическое изображение классификации межсетевых экранов на основе сетевой модели OSI

Существует два варианта исполнения межсетевых экранов – программный и программно-аппаратный. В свою очередь программно-аппаратный вариант имеет две разновидности: в виде отдельного модуля в коммутаторе или маршрутизаторе и в виде специализированного устройства.

Межсетевой экран не в состоянии решить все проблемы безопасности корпоративной сети. Имеется ряд ограничений в их использовании, а также существуют угрозы, от которых межсетевые экраны не могут защитить. Ниже представлены наиболее существенные ограничения в применении межсетевых экранов:

- неудовлетворительная защита от атак сотрудников компании;
- ограничение в доступе к нужным сервисам;
- ограничение пропускной способности;
- определенное количество остающихся уязвимых мест.

При подключении корпоративной или локальной сети к глобальным сетям при построении политики сетевой безопасности должны решаться следующие задачи:

- 1) защита локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;
- 2) скрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
- 3) разграничение доступа в защищаемую сеть из глобальной и из защищаемой сети в глобальную.

Часть задач по отражению наиболее возможных угроз для внутренних сетей могут решать межсетевые экраны. Использование межсетевых экранов дает возможность организовать внутреннюю политику безопасности сети предприятия, поделив всю сеть на сегменты, и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую.

Список использованных источников:

1. Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. – ИНФРА-М, 2011. – 416 с.
2. Лапонина О. Р. Межсетевое экранирование. — Бином, 2014. — 343 с.
3. Бобов М.Н. Методы использования трансляции адресов в межсетевых экранах. Труды БГУИР N 5, 2009.