ВОЕННО-КОСМИЧЕСКАЯ АКАДЕМИЯ ИМЕНИ А.Ф. МОЖАЙСКОГО

Кафедра № 27 Математического и программного обеспечения

УТВЕРЖДАЮ
Начальник 27 кафедры
полковник_____С.Войцеховский

«___» _____ 201_ г.

Автор: преподаватель 27 кафедры
Кандидат технических наук
майор С.Краснов

Лекция № 13

Тема: «МЕЖСЕТЕВЫЕ ЭКРАНЫ»

по дисциплине: «Защита информации»

Обсуждено и одобрено на заседании 27 кафедры
протокол № __ «____» _____ 201_ г.

Санкт-Петербург
201_

Содержание занятия и время

Введение – 5 мин.

Учебные вопросы (основная часть):

1. Предназначение и классификация МЭ – 30 мин.
2. Схемы подключения сегментных МЭ и технология сетевой трансляции адресов – 20 мин.
3. Обзор современных МЭ – 30 мин.

Заключение – 3-5 мин.

Литература:

Основная:

1. Войцеховский С.В., Воробьёв Е.Г. Методы и средства защиты компьютерной информации: учебно-методическое пособие. – СПб.: ВКА имени А.Ф. Можайского 2013. – 134 с.
2. Воробьев Е.Г. Защита информации в автоматизированных системах военного назначения. Учебное пособие – СПб, ВКА им.А.Ф. Можайского, 2007. – 252 с.

Дополнительная:

1. Вихорев С.В. Классификация угроз информационной безопасности. - http://www2.cnews.ru/comments/security/elvis_class.shtml
2. Войцеховский С.В., Марковский А.С., Палагушин В.А. Защита информации в автоматизированных системах. / Под ред. профессора Хомоненко А.Д. – Спб.:НТЦ им. Л.Т. Тучкова, 2005. – 149 с.

Материально техническое обеспечение:

1. Технические средства обучения: ПЭВМ, мультимедиа проектор, экран, программное обеспечение.
2. Приложения (слайды).
3. Наглядные средства обучения – доска, мел.

Организационно-методические указания:

Цель лекции: *Дать знания в области сетевого экранирования.*

Во введении сформулировать тему лекции, цель и название изучаемых вопросов. При этом произвести опрос курсантов по пройденному материалу.

Применяемым методическим приемом является рассказ.

В основной части сконцентрировать внимание курсантов на сетевом экранировании.

В заключительной части обобщить изложенный материал и осуществить контрольный опрос.

1. Перечислите основные межсетевые экраны?
2. В чем заключается суть механизма сетевого экранирования?
3. Охарактеризуйте программно-аппаратное сетевые экраны?

Отвечаю на вопросы по теме занятия, даю задание на самостоятельную подготовку.

Лекция № 11

«Защита информации с помощью межсетевых экранов»

В.1. Предназначение и классификация МЭ

В глобальной сети Интернет остро стоят вопросы информационной безопасности. Одним из методов защиты сетевых информационных ресурсов организации, имеющей выход в Интернет, является использование специальных программных (программно-аппаратных) средств, называемых Fire Wall (огненная стена) [16]. В отечественной литературе их принято называть межсетевыми экранами (МЭ). Иногда встречается название «брандмауэр», но сейчас этот термин используется редко.

Индустрия МЭ постоянно развивается. Вслед за развитием новых способов нарушения информационной безопасности создавались и новые технологии защиты, предотвращающие такие нарушения.

Межсетевые экраны первого поколения – *фильтры пакетов* – появились в конце 1980-х годов. В 1985 г. компания Cisco представила законченное решение фильтрующего маршрутизатора. Однако первые публикации, описывающие процесс экранирования, появились только в 1988 г.

В 1989–1990 годах была разработана архитектура МЭ второго поколения, известная как *МЭ уровня соединения*.

Третье поколение межсетевых экранов *прикладного уровня* разрабатывалось в США в конце 1980 начале 1990-х годов. Публикации, описывающие МЭ прикладного уровня, впервые появились в 1990–1991 годах.

Компания Check Point Software реализовала в 1994 г. первый коммерческий продукт, основанный на технологии *динамической фильтрации пакетов*.

Следующим толчком в развитии технологии стало появление МЭ Fire Wall-1 компании Check Point. Впервые МЭ имел дружественный графический интерфейс пользователя, облегчающий процесс настройки и обслуживания.

Начиная примерно с середины 1990-х годов, рынок продуктов межсетевых экранов получил бурное развитие и на сегодняшний день насчитывает более ста реализаций различных производителей. Сегодня ни одна организация, использующая Интернет, не обходится без использования МЭ или отдельных технологий межсетевого экранирования.

Современные коммерческие МЭ представляют собой сложные многофункциональные системы, использующие последние достижения в области информационных технологий и защиты информации. Сегодня МЭ представляют до 85 % всех используемых в локальных сетях средств защиты и по прогнозу некоторых аналитических компаний МЭ, поддерживающие технологию виртуальных частных сетей, длительное время будут составлять основу средств защиты информации при подключении организаций к сети Интернет (рис. 3.1).

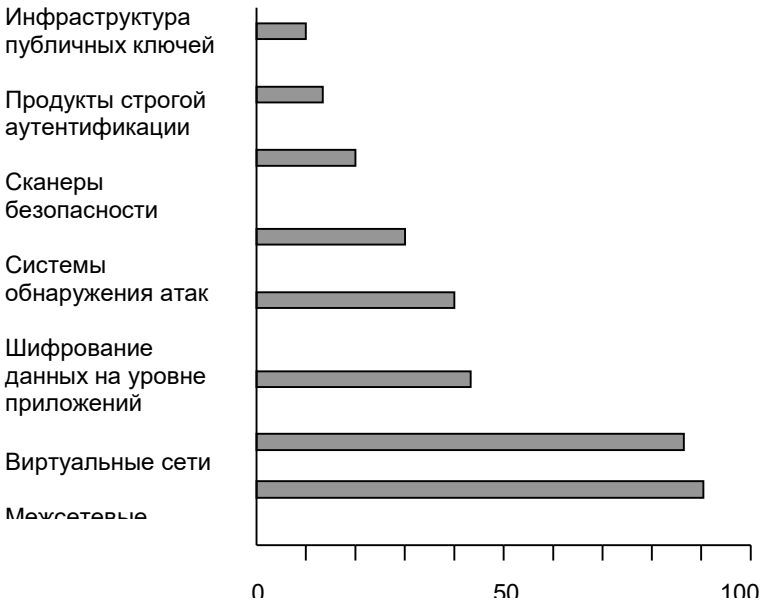

Рис. 3.1. Распределение продуктов безопасности

Функции сетевого экранирования

Межсетевой экран представляет собой программный или программно-аппаратный комплекс, реализующий функции фильтрации сетевого трафика (информационных потоков) между двумя и более компьютерными сетями по некоторому набору правил, определяемых политикой безопасности защищаемой сети (рис. 3.2) [16].

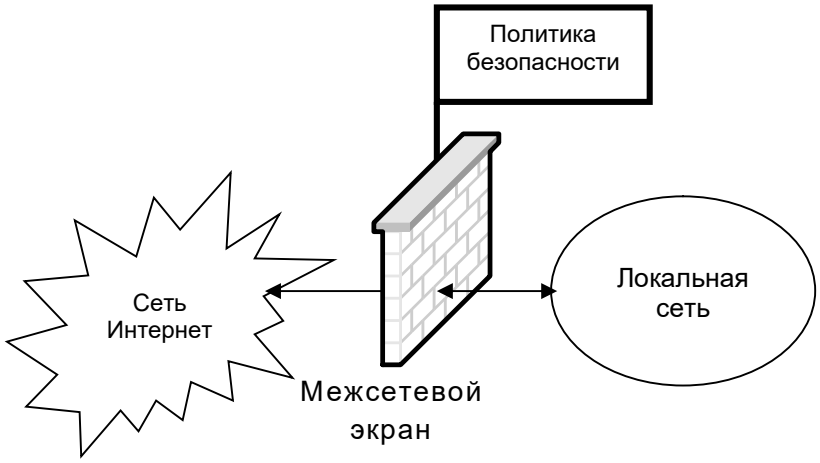

Рис. 3.2. Обобщенная схема межсетевого экранирования

Программные МЭ ориентированы на конкретную платформу (Windows, Solaris Sun и другие). Программно-аппаратные МЭ выполняются в виде «чёрного ящика», конфигурируемого через интерфейсы удалённого управления на основе собственных приложений либо с использованием стандартных интерфейсов (Web, SSH и другие). Преимуществами последних, по сравнению с программными МЭ, являются:

- в случае неполадок ОС, нарушений информационной безопасности не будет;
- простота эксплуатации;
- более высокая производительность и надёжность.

В большинстве случаев подключение локальных сетей к Интернету (и сетей между собой) осуществляется таким образом, что в точке соединения сетей существует возможность контроля всего сетевого трафика, проходящего между этими сетями. Исключение составляет случай, когда локальная сеть одновременно подключена к Интернету более чем одним соединением, например, для резервирования каналов связи или повышения пропускной способности.

МЭ позволяет значительно уменьшить, а в некоторых случаях и полностью исключить зону возможных рисков при подключении к потенциально опасным сетям, таким как Интернет (рис. 3.3) [16]. В идеальном случае МЭ должен блокировать все угрозы информационной безопасности, имеющие место

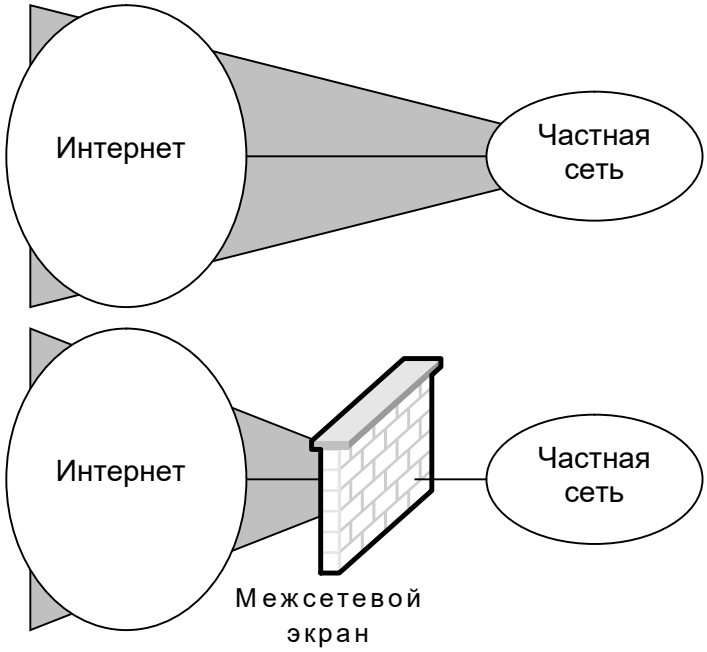

Рис. 3.3. Зоны риска незащищённой и защищённой частной сети

в Интернете, на своем внешнем сетевом интерфейсе.

Другими словами, МЭ – это компонент сетевой инфраструктуры, устанавливающий барьер безопасности между сетями или сетевыми сегментами. МЭ представляет собой устройство, частично реализующее политику безопасности сети организации. Межсетевой экран разделяет физически и логически две и более, как правило, IP-сети на сети с различными политиками безопасности. В большинстве случаев МЭ разделяет две сети, одна из которых является сетью защищаемой организации, а другая – Интернет.

Фильтрация трафика

Под *фильтрацией трафика* понимается возможность его блокирования (запрещения), разрешения или изменения. Такие действия и выполняет МЭ, обеспечивая защиту («экранирование») сети.

Говоря о МЭ, прежде всего подразумевают, что они используются в сети Интернет, которая основывается на стеке протоколов TCP/IP. Сети на основе протокола IP являются сетями с коммутацией пакетов. В таких сетях пакеты выступают единицей передачи данных между участниками сетевого обмена. Межсетевые экраны реализуют механизмы контроля доступа путем фильтрации всего входящего и исходящего трафика, пропуская только авторизованные данные.

Фильтры пакетов работают, применяя набор правил, установленных в ядре TCP/IP стека МЭ. Этот набор правил содержит определённые действия, которые будут применены ко всем входящим и исходящим пакетам.

Действие над поступающим на сетевой интерфейс или исходящим из него пакетом имеет одно из двух значений: запретить (deny) или разрешить (allow). Запрещение прохождения пакета выполняется одним из следующих способов:

1) пакет отбрасывается без каких-либо дополнительных действий;

2) пакет отбрасывается и отправителю посылается пакет с установленным флагом «сброс соединения». Это правило используется только для TCP-пакетов;

3) пакет отбрасывается и отправителю посылается сообщение – хост недостижим или порт недоступен.

Последние два способа запрещения пакетов позволяют создать видимость отсутствия средств защиты (фильтрации) на пути прохождения сетевых пакетов.

В ядре МЭ создаются и обрабатываются два списка – запрещенный список и список доступа. Сетевой пакет, проходящий через МЭ, должен пройти оба списка доступа. В большинстве МЭ применяется правило: что явно не разрешено, то запрещено. Некоторые фильтры пакетов, включенные в состав маршрутизаторов, используют другую политику: пакет должен быть явно запрещен или иначе он будет разрешен. По этой причине необходимо ясно понимать политику фильтрации, используемой в активном оборудовании и МЭ. При задании правил фильтра пакетов используют и более сложные подходы, реализующие многоуровневую иерархическую структуру.

Применение систем корпоративного и персонального экранирования

Классификация МЭ по типам защищаемых объектов приведена на рис. 3.4 [16]. Различают три основных типа МЭ: сегментные, персональные и встраиваемые.

Рис. 3.4. Классификация МЭ по типу защищаемых объектов

Под *сегментными* понимают МЭ, установленные на границе двух и более сетей. Они предназначены для контроля сетевых потоков между двумя и более сетями, т. е. выполняют защиту сетей. Сегментные МЭ позволяют контролировать весь сетевой трафик между сетями, к которым подключен МЭ.

Контроль трафика осуществляется на всех уровнях модели OSI, начиная с сетевого. Сегментный МЭ можно представить как сетевой маршрутизатор, который не только осуществляет маршрутизацию пакетов между сетями, но и выполняет анализ пакетов и информационных потоков на соответствие требованиям политики безопасности. Пакеты и информационные потоки, не удовлетворяющие этим требованиям, блокируются. Именно сегментные МЭ являются одним из основных средств обеспечения информационной безопасности.

Персональные МЭ защищают рабочие станции пользователей от внешних сетевых угроз и сетевых троянских программ. Персональные МЭ предназначены для защиты рабочих станций пользователей как отдельно подключенных к сети Интернет, так и функционирующих в составе локальных сетей. В последнем случае персональные МЭ создают дополнительный уровень защиты, в том числе и от внутренних угроз, и не исключают использования сетевых МЭ на границе локальной сети.

Среди персональных МЭ выделяют следующие разновидности экранов:

- пакетные фильтры,
- прокси-серверы,
- гибридные МЭ.

Пакетные фильтры отслеживают только сетевые пакеты на сетевом и транспортном уровне и не могут отслеживать соответствие пакетов и сетевых приложений. Пакетные фильтры требуют высокой квалификации пользователей.

Прокси-серверы отслеживают активность сетевых приложений. Такой подход не требует высокой квалификации пользователей и обеспечивает повышенный уровень защиты (по сравнению с пакетными фильтрами). Прокси-серверы могут иметь в своем составе прикладных посредников.

Гибридные персональные МЭ поддерживают функциональность и пакетных фильтров, и мониторов приложений, что позволяет реализовывать политику безопасности как на уровне сетевых приложений, так и на пакетном уровне.

Встраиваемые МЭ устанавливаются на прикладных серверах и предназначены для их защиты. Иногда возникает необходимость в усилении защиты прикладных служб, реализуемых одним или несколькими серверами. При этом использование сегментных МЭ может быть не оправдано по причине их высокой стоимости или условий эксплуатации (например, выделенный сервер на территории провайдера). В

этом случае можно использовать встраиваемые МЭ, которые функционируют на одной платформе с защищаемыми серверами, обеспечивая их защиту. Низкая стоимость встраиваемых МЭ позволяет установить их на каждый защищаемый сервер.

Встраиваемые МЭ обеспечивают защиту по принципу персональных фильтрующих МЭ и предоставляют более широкие возможности управления (удаленное управление, резервное копирование, временные ограничения политики безопасности и др.) и анализа событий. Но в отличие от персональных, они не обеспечивают интерактивности взаимодействия с администратором прикладного сервера.

Особенности межсетевого экранирования на различных уровнях модели OSI

Все межсетевые экраны функционируют на основе информации, получаемой от различных уровней эталонной модели OSI, и чем выше уровень OSI, на основе которого построен межсетевой экран, тем выше уровень защиты, им обеспечиваемый. На рис.3.5 представлены уровни модели OSI (самый низкий – канальный, высокий – прикладной) и классификация сегментных МЭ.

Выделяют следующие типы сегментных МЭ [16]: управляемые коммутаторы, статические и динамические фильтры пакетов, инспекторы состояния, посредники сеансового уровня, посредники прикладного уровня и МЭ экспертного уровня.

Управляемые коммутаторы попадают под определение МЭ, но действуют они на самом нижнем уровне модели взаимодействия (канальном), что не позволяет управлять на уровне протокола IP. Тем не менее, появление коммутаторов 3-го уровня, стандартизация протоколов коммутации, расширение возможностей коммутаторов 2-го уровня позволяют использовать возможности коммутаторов в целях повышения безопасности локальных сетей и на более высоких уровнях – на сетевом и транспортном.

Технология виртуальных локальных сетей VLAN (Virtual Local Area Network) позволяет создавать группы узлов сети, трафик которых полностью изолирован от других узлов сети. Применение VLAN помогает решать две задачи. Во-первых, это повышение производительности сети и, во-вторых, как уже говорилось, обеспечение безопасности за счет физического разделения трафика между сегментами сети.

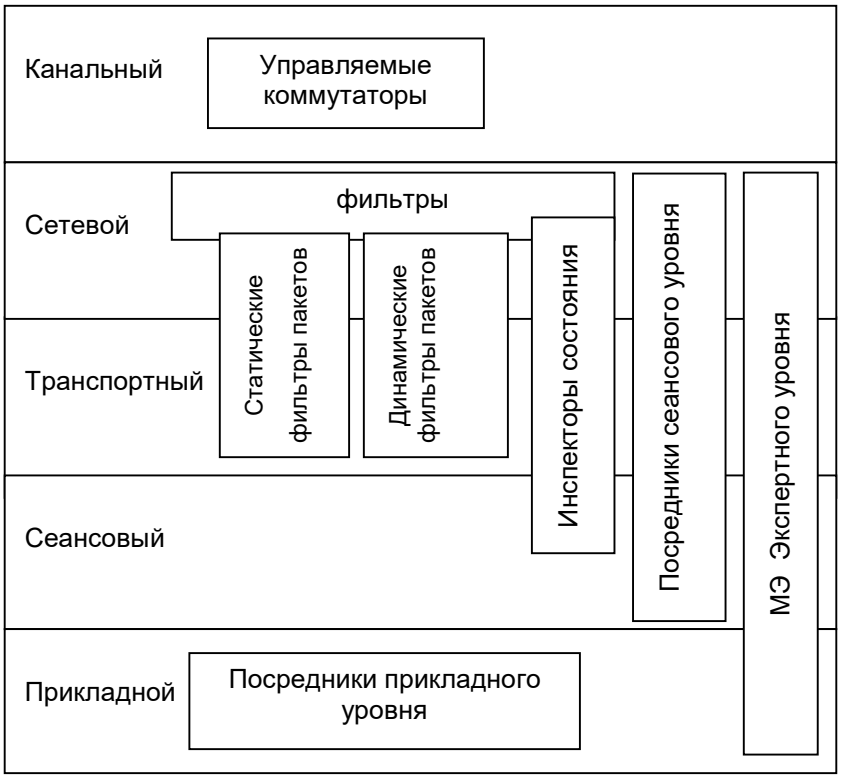

Рис. 3.5. Уровни модели OSI

Выделяют следующие способы построения виртуальных локальных сетей на базе коммутаторов:

- использование номеров подсетей сетевого уровня;
- группировка портов;
- группировка MAC-адресов;
- группировка протоколов сетевого уровня;

• добавление к кадрам канального уровня меток виртуальных сетей.

Второй и третий способы являются универсальными, их поддерживают большинство моделей коммутаторов Cisco, 3Com, Bay Networks, Cabletron. При группировке портов узлы сети объединяются в виртуальные группы по портам коммутатора. Каждой из создаваемых сетей VLAN назначаются определенные порты коммутатора (рис. 3.6.).

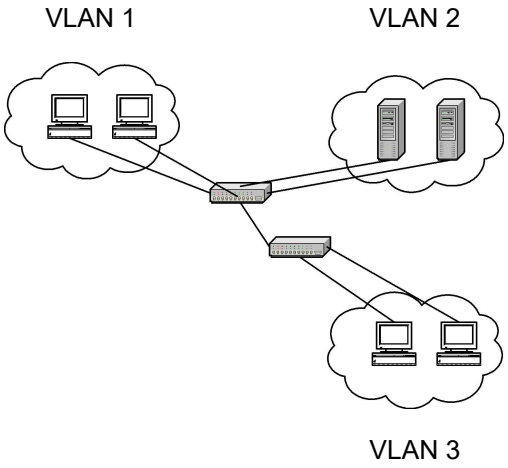

Рис. 3.6. Группировка портов коммутатора

При построении сети способом группировки MAC-адресов параметром разграничения выступает MAC-адрес сетевого адаптера компьютера (IP-узла), который является уникальным. Зная MAC-адреса всех компьютеров, можно создать группы и определить правила прохождения трафика между ними.

Положительные моменты: при реализации политики безопасности в корпоративной сети управляемые коммутаторы могут быть мощным и достаточно дешевым решением проблемы безопасности. Особенно полезны управляемые коммутаторы для разграничения доступа внутри организации с жесткой и статичной политикой безопасности. К тому же, в большинстве компаний коммутаторы составляют основу сети, и не стоит забывать о дополнительных их возможностях.

Основные недостатки использования управляемых коммутаторов [16]:

- отсутствие или ограничение возможностей фильтрации трафика на сетевом и более высоких уровнях модели OSI;
- отсутствие механизмов аутентификации (процесс, гарантированно определяющий подлинность объекта на основе предъявляемых идентификаторов и использования специальных протоколов и схем);
- сложность управления и определения правил фильтрации.

В ряде случаев сегментация с использованием технологии VLAN, поддерживаемой управляемыми коммутаторами, является достаточным решением при организации разграничения доступа внутри локальной сети.

Статические фильтры пакетов – первое поколение технологии МЭ – анализируют сетевой трафик на сетевом и транспортных уровнях. Каждый IP-пакет проверяется на соответствие набору правил, определяющих разрешенные потоки данных. Если доступ разрешен, сетевой пакет будет маршрутизирован через МЭ как определенный правилами в таблице маршрутизации МЭ. Поскольку такой МЭ требует минимальных вычислительных затрат и обеспечивает самую высокую производительность, его часто используют в таких аппаратных решениях, как IP-маршрутизаторы.

МЭ на основе статической фильтрации пакетов имеют следующие достоинства:

• простота реализации и широкая доступность, как в программном исполнении, так и аппаратном (в составе маршрутизаторов);

• более высокая производительность по сравнению с другими типами МЭ, поскольку выполняют меньшее количество операций в процессе анализа;

• не требуется специальное конфигурирование клиентских компьютеров;

• в сочетании с сетевой трансляцией адресов позволяет скрыть внутренние адреса сети от внешних пользователей.

МЭ на основе статической фильтрации пакетов имеют следующие недостатки:

• не интерпретируют прикладной уровень модели OSI, не отслеживают текущие сессии. Поэтому они обеспечивают меньшую защищенность, чем МЭ прикладного уровня или уровня соединения;

• имеют ограниченные системы аудита и предупреждений или вообще не имеют их;

• из-за сложности реализации большинства прикладных служб возникают сложности определения разрешенных и запрещенных списков правил, что усложняет их администрирование (настройку и обслуживание).

Фильтры пакетов являются неотъемлемой частью МЭ экспертного уровня.

МЭ динамической фильтрации пакетов работают на транспортном уровне модели OSI, они позволяют модифицировать (корректировать) базу правил «на лету». Эта технология изначально разрабатывалась для поддержки транспортного протокола UDP. Транспортный протокол UDP обычно используется при небольших информационных запросах и ответах на прикладном уровне.

МЭ динамической фильтрации ассоциирует все UDP-пакеты с неким виртуальным соединением (протокол UDP не определяет понятие соединения). Если МЭ обнаруживает ответный пакет, то устанавливается виртуальное соединение, и пакету разрешается проходить через МЭ. Информация, ассоциированная с виртуальным соединением, обычно запоминается на короткий промежуток времени, и если в этот промежуток времени не получен (обнаружен) ответный пакет, то виртуальное соединение разрывается (ликвидируется).

МЭ динамической фильтрации имеют такие же преимущества и недостатки, как и первое поколение МЭ – МЭ статических фильтров пакетов с одним исключением – дополнительно они не пропускают незапрашиваемые (согласно оценок виртуального соединения) UDP-пакеты. МЭ пропускает первый пакет UDP во внутреннюю сеть. Ответный пакет должен содержать соответствующий адрес назначения и номер порта.

Динамические фильтры, как МЭ, в настоящее время не используют. Принципы, заложенные в динамической фильтрации, реализованы и значительно расширены в инспекторах состояния.

Инспекторы состояния (шлюзы сеансового уровня) осуществляют фильтрацию сетевых пакетов с учетом информации о текущей фазе соединения на транспортном уровне модели OSI. Инспектор состояний гарантирует, что ни один сетевой пакет не будет пропущен, если он не принадлежит ранее установленному соединению. Подобно фильтрам пакетов, инспекторы состояния используют набор правил, которые установлены в ядре TCP/IP МЭ.

Для подтверждения TCP-сессии МЭ исследует каждый процесс установки соединения, следующий за законным рукопожатием. Кроме того, пакеты данных не отправляются, пока процесс рукопожатия не будет закончен. МЭ поддерживает таблицу состоявшихся соединений (в которой содержится полная информация о состоянии сессий: номера последовательностей TCP/UDP, IP-адреса, портов) и позволяет сетевым пакетам проходить тогда, когда информация о пакете соответствует фазе соединения. Как только соединение закрывается, записи о нем удаляются из таблицы, и виртуальное соединение между двумя транспортными уровнями закрывается.

МЭ на основе инспекторов состояний имеют следующие преимущества:

• инспекторы состояний обычно быстрее, чем МЭ прикладного уровня, поскольку выполняют меньшее количество операций;

• инспекторы состояний контролирует сессию в целом, что обеспечивает большую защищенность по сравнению с фильтрами пакетов;

• практически исключена подделка трафика и отдельных пакетов TCP;

• гибкость создания правил политики безопасности (по сравнению с пакетными фильтрами), а также способность защиты от большинства DDos-атак.

Недостатками МЭ на основе инспекторов состояний являются:

• полнофункциональная инспекция возможна только для TCP;

• не обеспечена проверка вышестоящих протоколов;

• ограниченные возможности аудита событий, но по сравнению с пакетными фильтрами они могут связывать сетевой пакет с протоколом прикладного уровня путем построения ограниченных форм состояний сессии;

• из-за непонимания протоколов прикладного уровня не имеют дополнительных возможностей;

• из-за сложности реализации большинства прикладных служб возникают сложности определения разрешенных и запрещенных списков доступа (правил).

Посредники сеансового уровня работают на сеансовом уровне модели OSI (этот уровень в стандартном стеке протоколов Интернет отсутствует). Они позволяют аутентифицировать клиентов, передавать данные по защищенному каналу и иметь ряд дополнительных возможностей, отсутствующих в пакетных фильтрах.

Наиболее известным примером посредника сеансового уровня является посредник SOCKS5. При запросе соединения с некоторым узлом Интернет, SOCKS5 проводит аутентификацию клиента и проверяет его права на доступ к запрашиваемому узлу по запрашиваемому прикладному протоколу (на основании номера порта TCP/UDP). При успешной аутентификации пользователя SOCKS5 устанавливает соединение с запрашиваемым узлом, что обеспечивает единую точку входа в сеть с

обеих сторон сервера SOCKS5. SOCKS5 позволяет передавать данные, как в открытом виде, так и по защищенному протоколу, например SSL.

Недостатком использования посредника SOCKS5 является необходимость установки на каждое рабочее место клиентской части SOCKS5, если, конечно, прикладные приложения сами не поддерживают работу через SOCKS5. Кроме того, нужно отметить, что поскольку клиентская часть SOCKS5 работает на основе перехвата вызовов сетевого API ОС, то по ряду причин не все приложения будут поддерживать работу через SOCKS5.

Преимущество SOCKS5 состоит в том, что он позволяет полноценно управлять доступом к различным ресурсам (адрес: порт) закрытой и общедоступной сетей на основе строгой аутентификации и при этом поддерживает транспортные протоколы TCP и UDP.

Посредники прикладного уровня – технология МЭ, которая проверяет информационные потоки на корректность данных на прикладном уровне модели OSI. Дополнительно на этом уровне МЭ прикладного уровня могут контролировать различные характеристики защищенности, присущие только прикладному уровню, такие как пароль пользователя и запрашиваемые объекты протоколов. Посредники оперируют не пакетами, а информационными массивами в виде команд и их параметров, результатами выполнения команд, различными высокоуровневыми объектами - файлами, элементами баз данных и др.

Большинство МЭ прикладного уровня включают специальное программное обеспечение и сервис-посредники (proxy services). Сервис-посредники – программы специального назначения, которые управляют трафиком через МЭ для определенных служб. МЭ прикладного уровня позволяют блокировать потенциально опасные компоненты и команды прикладного протокола.

Основными преимуществами *сервис-посредников являются*:

• интерпретация и усиление защиты высокоуровневых прикладных протоколов, таких как HTTP и FTP;

• блокирование напрямую установленных соединений между внешними серверами и внутренними хостами;

• перенаправление внешних запросов на другие серверы внутренних служб;

• широкий набор учетных данных для отчетности по сравнению с другими типами МЭ (идентификатор пользователя, время и продолжительность соединения для каждой пары адресов, имена и характеристики запрашиваемых объектов, статистика посещения узлов и запрашиваемых объектов, распределение затраченного сетевого времени между приложениями и пользователями и ряд других).

Недостатки *сервис-посредников*:

• поскольку они прослушивают тот же порт, что и сам прикладной сервер, то не всегда есть возможность расположения сервера и МЭ на одном и том же компьютере;

• значительное время обработки, поскольку входящие данные обрабатываются дважды - приложением и его посредником;

• для каждого прикладного протокола, пропускаемого через МЭ, должен быть разработан собственный сервис-посредник.

Сервис-посредники обеспечивают самый высокий уровень защиты из всех типов МЭ, но имеют самую низкую производительность.

МЭ экспертного уровня реализуют все вышеперечисленные технологии МЭ, за исключением фильтрации MAC-адресов, используемых в некоторых типах управляемых коммутаторов. Практически все коммерческие МЭ относят именно к этому классу.

Алгоритмы работы МЭ экспертного уровня имеют сложный многоуровневый характер и отличаются у различных фирм-производителей МЭ, однако можно выделить следующие черты, присущие всем МЭ экспертного уровня:

• имеют набор прикладных посредников;

• должны поддерживать технологию инспекции состояния этих каналов связи;

• для увеличения защищенности самой ОС, а также из-за сложности алгоритмов обработки заменяют сетевой стек ОС на собственный. Кроме того, осуществляют действия по настройке имеющихся механизмов защиты ОС, например, настройке прав доступа к объектам ОС, включению механизмов аудита и др.;

• имеют встроенные механизмы обнаружения и защиты от типовых сетевых атак типа «отказа в обслуживании»;

• предоставляют возможности централизованного управления и интеграции с системами управления сетями;

• обеспечивают режимы повышенной надежности за счет объединения однотипных продуктов в отказоустойчивый кластер;

• поддерживают усиленные схемы аутентификации;

• имеют развитую систему аудита и уведомления о событиях безопасности;
• поддерживают технологию VPN.

В.2. Схемы подключения сегментных МЭ

Для защиты АС применяются различные схемы подключения сегментных МЭ. Наибольшую известность из них получили следующие:

- на основе фильтрующего маршрутизатора;
- на основе двухпортового шлюза (Dual-homed);
- на основе демилитаризованной зоны;
- на основе экранирующего экрана (бастион-хост);
- на основе экранирующей подсети;

МЭ на основе ***фильтрующего маршрутизатора*** является самым распространённым и простым в реализации. Он состоит из фильтрующего маршрутизатора, расположенного между ЛВС и сетью Интернет. Он может осуществлять фильтрацию входящих и исходящих пакетов на основе анализа их адресов и портов.

МЭ на основе ***двухпортового шлюза*** *(Dual-homed)* означает, что МЭ имеет два сетевых адаптера подключённых к двум различным сетям. Это наиболее распространённая схема подключения МЭ. Со стороны внешней сети МЭ подключён к маршрутизатору (чаще всего провайдера). После МЭ располагают сетевой коммутатор или концентратор (см. рис.3.7). Внутренний маршрутизатор (на рис 3.8, 3.9, 3.10 маршрутизаторы обозначены как «М») используется в больших корпоративных сетях или для усиления ПБ.

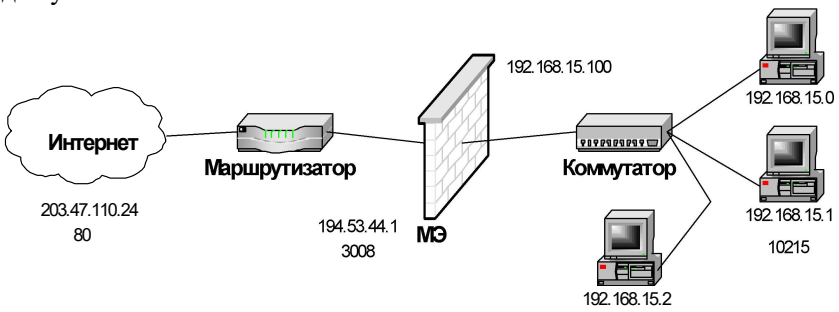

Рис. 3.7. Подключение МЭ по схеме двупортового шлюза (Dual-homed) с динамической трансляцией адресов

МЭ на основе *демилитаризованной зоны* – это МЭ с несколькими сетевыми адаптерами, с возможностью установления различных ПБ между подключаемым к ним сетям, а также с образованием так называемой демилитаризованной зоны (DMZ-demilitarized zone). Как правило, в которой размещаются службы, которые должны быть доступны и клиентам сети Интернет и клиентам ЛВС. В демилитаризованной зоне определяются менее жёсткие требования к сетевой безопасности, но достаточные для организации защиты от внешних угроз. МЭ на основе демилитаризованной зоны, имеющий три сетевых адаптера, изображен на рис. 3.8.

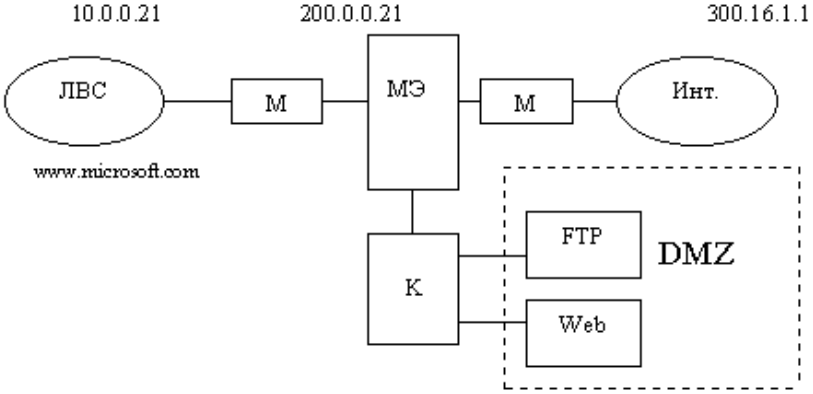

Рис.3.8. Подключение МЭ по схеме демилитаризованная зона со статической трансляцией адресов

МЭ на основе *экранирующего экрана* (ранее в технической литературе его называли бастион-хост) – это МЭ подключенный только ко внутренней сети и имеющий один сетевой интерфейс (см. рис.

3.9). Маршрутизатор настраивается так, чтобы весь входящий трафик отправлялся на МЭ, а в ЛВС в качестве шлюза указывается адрес интерфейса МЭ. Данная схема подключения имеет меньшую защищённость, чем на основе МЭ с несколькими сетевыми интерфейсами поэтому используется редко.

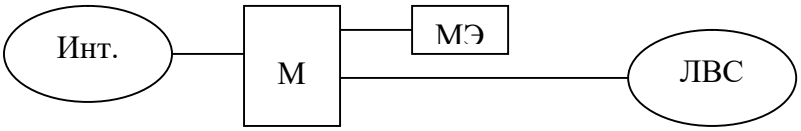

Рис. 3.9. Подключение МЭ по схеме экранирующий экран

МЭ на основе *экранирующая подсеть* по сравнению с предыдущей схемой подключения добавляет дополнительный уровень безопасности путём внесения дополнительного маршрутизатора для улучшения изоляции защищённой сети от Интернет (см. рис. 3.10). Два экранирующих маршрутизатора образуют внутреннюю фильтрующую подсеть, которая может выполнять функции демилитаризованной зоны.

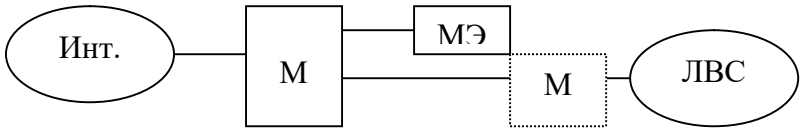

Рис. 3.10. Подключение МЭ по схеме экранирующая подсеть

Технология сетевой трансляции адресов (NAT – Network address translation) широко используется в большинстве МЭ. При использовании NAT МЭ выступает посредником между двумя IP-узлами, организуя два канала передачи данных. Он взаимодействует с внешним IP-узлом от имени внутреннего, но со своим IP-адресом, что позволяет скрыть внутреннюю структуру сети и иметь всего один зарегистрированный внешний IP-адрес. Сетевая трансляция адресов осуществляется в следующих режимах:

1. *Динамическом* (трансляция на уровне портов) – МЭ имеет один внешний IP адрес (см. рис. 3.7). МЭ при обращении к нему клиента выделяет ему уникальный порт транспортного протокола (TCP, UDP) для внешнего IP адреса. Выделяемый пул портов может составлять 65535 портов, но чаще всего 10000 – 20000 портов. В ряде ОС Unix динамический режим трансляции называют маскарадингом. В основном он предназначен для сетей, хосты которых выступают клиентами сети Интернет.
2. *Статическом* – внешнему интерфейсу МЭ назначается столько зарегистрированных IP адресов, сколько хостов имеется во внутренней сети (см. рис. 3.8). Каждому хосту внутренней сети ставится в соответствие уникальный внешний IP адрес МЭ. Он используется, если хосты внутренней сети являются серверами Интернет.
3. *Комбинированном* – может использовать сразу несколько режимов. Его применяют в сетях, где необходимо обеспечить работу и клиентов и серверов расположенных в защищённой сети. Далеко не все МЭ поддерживают комбинированный режим трансляции адресов.

В.3. Обзор современных межсетевых экранов

На сегодняшний день рынок МЭ представлен более 50-ю компаниями-производителями. Наблюдается бурный рост и на рынке персональных экранов. Продукты даже одного производителя могут сильно отличаться от версии к версии или в зависимости от платформы, что также затрудняет выбор конкретного продукта [16]. В таблице 3.2 приведены наиболее известные модели МЭ.

Только серийные МЭ

1. Межсетевой экран ИВК Кольчуга - по 2 классу для МЭ и по 2 уровню для контроля НДВ
2. Программный комплекс «Межсетевой экран «ЗАСТАВА М» для ОС МСВС 3.0 – по 2 классу для МЭ и по 2 уровню НДВ.
3. пециальное программное обеспечение межсетевой экран «Z-2», версия 2.6 на соответствие ЗБ 17801922.Z-2.002.ЗБ.0.7.0 и имеет оценочный уровень доверия ОУД 4 (усиленный) - РД «Безопасность информационных технологий. Критерии оценки

безопасности информационных технологий» и по 2 классу для МЭ и по 2 уровню для НДВ.

4. Программный комплекс «Межсетевой экран «ЗАСТАВА-S» для ОС Solaris 9 и Windows 2003 – по 2 классу для МЭ и по 2 уровню НДВ.
5. Межсетевой экран Cisco ASA-5505 - по 3 классу для МЭ и на соответствие ТУ (серия).
6. Программно-аппаратный комплекс межсетевой экран «WatchGuard Firebox» с программным обеспечением «Fireware OS» версии 11.10.7 Update 1 - межсетевой экран, предназначенный для защиты информации, не содержащей сведений, составляющих государственную тайну, соответствует 3 классу защищенности для МЭ
7. Межсетевой экран ССПТ-2 версии 1.3 - по 3 классу для МЭ и 3 уровню контроля НДВ
8. Программный комплекс межсетевой экран «Ideco ICS 3» - на соответствие ТУ, 4 класс РД МЭ, 4 уровень - по РД НДВ (может использоваться для защиты перданных до 2 класса включительно)
9. Программный комплекс «Межсетевой экран «ЗАСТАВА-SI», версия 5.3, функционирующий в среде операционной системы Solaris 10 - по 2 классу РД МЭ и по 3 уровню РД НДВ
10. Программный комплекс «Межсетевой экран «ЗАСТАВА-AL», версия 5.3, функционирующий в среде операционной системы ALT Linux - по 2 классу РД МЭ и по 3 уровню РД НДВ с ограничениями
11. Межсетевой экран и система обнаружения вторжений «Рубикон» - на соответствие требованиям к МЭ (ИТ.МЭ.А2.ПЗ) и СОВ (ИТ.СОВ.С2.ПЗ)
12. Программный межсетевой экран «Интернет Контроль Сервер» - на соответствие РД МЭ по 4 классу защищенности с ограничениями
13. Межсетевой экран Altell NEO версии 1.5– по 2 классу для МЭ и 2 уровню РД НДВ
14. Межсетевой экран серии Cisco ASA 55xx (модели: ASA 5512, ASA 5515, ASA 5525, ASA 5545, ASA 5555, ASA 5585) с установленным программным обеспечением Cisco ASA Software версии 9.1 - на соответствие РД МЭ по 3 классу
15. Межсетевой экран FortiGate с установленным программным обеспечением 5.0 (версии исполнения: FortiGate-40C-LENC/FortiGate-80C-LENC/FortiGate-100D-LENC/FortiGate-300C-LENC/FortiGate-600C-LENC/FortiGate-1000C-LENC/FortiGate-3040B-LENC/FortiGate-3950B-LENC/FortiGate-5101C-LENC) - на соответствие РД МЭ по 3 классу, РД НДВ по 4 уровню контроля
16. Межсетевой экран и систем обнаружения вторжений Рубикон-К на соответствие требованиям к МЭ и СОВ (ИТ.СОВ.С4.ПЗ) - по 3 классу защищенности, НДВ - по 4 уровню контроля
17. Межсетевой экран Kerio Control с версией программного обеспечения 8.2.0. - по 3 классу РД МЭ и 4 уровню по РД НДВ
18. Межсетевой экран Киберсейф: Межсетевой экран - на соответствие РД НДВ по 4 уровню контроля и РД МЭ по 3 классу
19. Межсетевой экран StoneGate Firewall версия 5.3 - на соответствие РД МЭ по 2 классу и РД НДВ по 4 уровню

Отметим, что в последнее время на российском рынке появилось большое количество как сегментных, так и персональных МЭ отечественного производства. Некоторые выпускаются большими сериями, некоторые – в единичных экземплярах. И хотя почти все они уступают общеизвестным мировым лидерам в области МЭ по производительности, однако по остальным техническим параметрам вполне конкурентоспособны с аналогичными западными образцами, а по такому показателю как цена выглядят намного привлекательнее.

Так известно, что большинство представленных на российском рынке продуктов американского производства имеющих встроенные средства криптографической защиты информации (СКЗИ) поставляются с криптоалгоритмом симметричного шифрования DES с длиной ключа 56 бит. Он имеет 2^{56} всех возможных значений (большим корпорациям потребуется несколько минут для его взлома, а хакеру одиночке несколько десятков лет). Для приобретения СКЗИ с более криптостойким алгоритмом 3 DES с длиной ключа 168 бит иностранным компаниям необходимо получать специальное

разрешение Государственного департамента США [24]. В сравнении с ними во многих отечественных МЭ применяется криптоалгоритм ГОСТ 28147-89 с длиной ключа 256 бит (2^{256} возможных значений), на сегодняшний день взломать такой криптоалгоритм практически не возможно.

Высокая сложность МЭ и их большое разнообразие делают выбор МЭ для защиты АС не простой задачей. Сказать, что «этот» МЭ однозначно лучше остальных будет не правильно. Кроме того, компании производители постоянно совершенствуют свои продукты, улучшая их производительность, расширяя функциональность, повышая управляемость и т. п. Поэтому функциональность и свойства, присутствующие сегодня только в одном МЭ, завтра будут реализованы и в остальных.

Все современные МЭ достаточно хорошо справляются со своей основной задачей - защитой внутренней сети от различных угроз со стороны внешней сети и могут выполнять ряд дополнительных функций, таких как трансляция сетевых адресов, антивирусная защита и т.п.

В качестве инструмента МЭ обладает рядом характеристик, позволяющих в зависимости от конкретной ситуации предпочесть тот или иной МЭ. Наиболее важными характеристиками МЭ являются его стоимость, производительность, простота использования, расширяемость и функциональность. Основные технические характеристики МЭ приведены в таблице 3.2. Большое значение имеют также репутация производителя (как долго находится в эксплуатации, перспективы дальнейшего развития МЭ), поддерживаемая программно-аппаратная платформа, обеспечиваемый уровень защищенности согласно требований руководящих документов ФСТЭК России и др.

Ещё одним немаловажным плюсом, при выборе МЭ, в направлении отечественных продуктов является то, что почти все они имеют действующие сертификаты ФСТЭК России (см. табл. 3.1, 3.2). Причём, что немаловажно, отечественные МЭ, как правило, имеют сертификат на всю серию данных продуктов, а зарубежные только на отдельную партию из десятков единиц. Сертификат выдаётся сроком на три года и по истечении этого времени он может быть продлён. Информацию о выданных сертификатах на конкретные средства защиты информации от несанкционированного доступа можно получить на Интернет-сайте www.gtk.lissi.ru.

Таблица 3.4 Сравнительные характеристики сегментных МЭ

Производитель модель	Макс. производительность Mbit/s	класс	Минимальная стоимость в у. е.	Метод шифрования, маскирования IP-трафика	версия	Сертификат ГТК / класс защиты
1	2	3	4	5	6	7
Check Point FireWall-l	100	Enterprise	2995	DES 40, 56, 168 RSA 512/1024	4.0 SP3	На партию / 3
Cisco IOS Firewall	10	SOHO/ Enterprise	850	DES 40, 56, bit (аппаратно или программно) CISCO PIX Ravlin encr. card	12.0	На партию / 4
Cisco PIX 520 Firewall	1000	Enterprise	9400	DES 56, 112, 186 bit (аппаратно или программно) CISCO PIX Ravlin encr. card	4.2	Разовый / 3
ОАО ЭЛВИС+ ЗАСТАВА 3.3	30-90	Enterprise	4040	DES 56, 112, 186 bit RSA 512/1024 (Другие)	3.3	Да / 3
ОАО ИнфоТеКС VipNet Office Firewall	15-18	SOHO/ Enterprise	300	DES 40, 56, 168 RSA 512/1024 ГОСТ28147-89	-	Да / 3
ООО АМИКОН ФПСУ-IP	90	SOHO/ Enterprise	1880	Свой, ГОСТ28147-89	1.82	Да / 3

Примечание: Все параметры указаны из информационных материалов производителей или их представителей.

Если требуется обеспечить максимальную производительность, то следует выбирать Cisco PIX Firewall, (однако это самое дорогое решение $9400) или CheckPoint Firewall-1 ($2995). Если требуется не дорогое решение, не требующее высокой производительности, то оптимальным будет VipNet Office Firewall ($300) и наконец оптимальным выбором в соотношении цена – качество выглядит ФПСУ-IP ($1880) компании ООО АМИКОН.

Приходим к следующим выводам:

1. Однозначного решения проблемы выбора МЭ не существует. В каждом конкретном случае выбор определяется экономическими и политическими соображениями (ПБ организации), требованиями заказчика и средой функционирования.
2. Для предприятий и организаций работающих с информацией, представляющей государственную тайну и для всех государственных учреждений нет иного пути, кроме изначальной ориентации на отечественных производителей МЭ, имеющих соответствующие лицензии и сертификаты Гостехкомиссии России. Причём в соответствии с [8] для защиты конфиденциальной информации, передаваемой по каналам связи между АС, если каналы связи выходят за пределы контролируемой зоны, необходимо использовать защищенные каналы связи, включая защищенные волоконно-оптические линии связи или сертифицированные криптографические средства защиты.
3. Для негосударственных предприятий и организаций документ [8] носит рекомендательный характер, и они могут использовать для защиты своих информационных ресурсов (составляющих коммерческую, банковскую тайну и т.д.) любые МЭ, в том числе и иностранного производства. Тут на первый план выходят такие параметры, как стоимость, функциональность, качество, производительность, криптостойкость, трудоемкость обслуживания, совместимость с уже имеющимся парком оборудования и.т.д.

Старший преподаватель 27 кафедры
подполковник С.Краснов