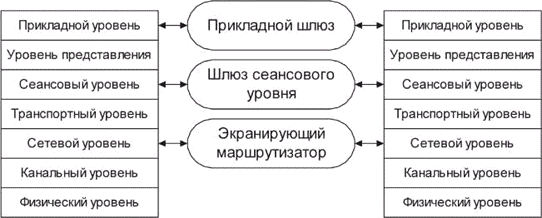
Лекция №22. Особенности функционирования межсетевых экранов на различных уровнях модели ОSI и схемы защиты.

# 1.Особенности функционирования межсетевых экранов на различных уровнях модели ОSI

МЭ поддерживают безопасность межсетевого взаимодействия на различных уровнях модели QSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Поэтому комплексный МЭ удобно представить в виде совокупности неделимых межсетевых экранов, каждый из которых ориентирован на отдельный уровень модели QSI.

Чаще всего комплексный экран функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели. Соответственно, различают такие неделимые МЭ (рис. 1), как:

* экранирующий маршрутизатор;
* шлюз сеансового уровня;
* шлюз прикладного уровня (экранирующий шлюз).

Используемые в сетях протоколы не полностью соответствуют эталонной модели OSI, поэтому экраны перечисленных типов при выполнении своих функций могут охватывать и соседние уровни эталонной модели.

**Рис. 1. Типы межсетевых экранов, функционирующих на отдельных уровнях модели OSI**

Например, прикладной экран может осуществлять автоматическое зашифровывание сообщений при их передаче во внешнюю сеть, а также автоматическое расшифровывание криптографически закрытых принимаемых данных. В этом случае такой экран функционирует не только на прикладном уровне модели OSI, но и на уровне представления.

Шлюз сеансового уровня при своем функционировании охватывает транспортный и сетевой уровни модели OSI. Экранирующий маршрутизатор при анализе пакетов сообщений проверяет их заголовки не только сетевого, но и транспортного уровня.

Межсетевые экраны указанных типов имеют свои достоинства и недостатки. Многие из используемых МЭ являются либо прикладными шлюзами, либо экранирующими маршрутизаторами, не обеспечивающими полной безопасности межсетевого взаимодействия. Надежную же защиту обеспечивают только комплексные межсетевые экраны, каждый из которых объединяет экранирующий маршрутизатор, шлюз сеансового уровня, а также прикладной шлюз.

## 1.1 Экранирующий маршрутизатор

Экранирующий маршрутизатор (Screening Router, называемый также пакетным фильтром (Packet Filter) предназначен для фильтрации пакетов сообщений и обеспечивает прозрачное взаимодействие между внутренней и внешней сетями. Он функционирует на сетевом уровне эталонной модели ОSI, но для выполнения своих отдельных функций может охватывать и транспортный уровень эталонной модели.

Решение о том, пропустить или отбраковать данные, принимается для каждого пакета независимо на основе заданных правил фильтрации. Для принятия решения анализируются заголовки пакетов сетевого и транспортного уровней (рис. 2).

***Рис. 2. Схема функционирования пакетного фильтра***

В качестве анализируемых полей IP- и ТСР- (UDР-) заголовков каждого пакета могут использоваться:

* адрес отправителя;
* адрес получателя;
* тип пакета;
* флаг фрагментации пакета;
* номер порта источника;
* номер порта получателя.

Первые четыре параметра относятся к IP-заголовку пакета, а следующие - к ТСР- или UDP-заголовку. Адреса отправителя и получателя являются IP-адресами. Эти адреса заполняются при формировании пакета и остаются неизменными при передаче его по сети.

Поле типа пакета содержит код протокола ICMP, соответствующего сетевому уровню, либо код протокола транспортного уровня (ТСР или UDP), к которому относится анализируемый IP-пакет.

Флаг фрагментации пакета определяет наличие или отсутствие фрагментации IP-пакетов. Если флаг фрагментации для анализируемого пакета установлен, то данный пакет является подпакетом фрагментированного IP-пакета.

Номера портов источника и получателя добавляются драйвером TCP или UDP к каждому отправляемому пакету сообщения и однозначно идентифицируют приложение-отправитель, а также приложение, для которого предназначен этот пакет. Для возможности фильтрации пакетов по номерам портов необходимо знание принятых в сети соглашений относительно выделения номеров портов протоколам высокого уровня.

При обработке каждого пакета экранирующий маршрутизатор последовательно просматривает заданную таблицу правил, пока не найдет правила, с которым согласуется полная ассоциация пакета. Здесь под ассоциацией понимается совокупность параметров, указанных в заголовках данного пакета. Если экранирующий маршрутизатор получил пакет, не соответствующий ни одному из табличных правил, он применяет правило, заданное по умолчанию. Из соображений безопасности это правило обычно указывает на необходимость отбраковки всех пакетов, не удовлетворяющих ни одному из других правил.

Пакетные фильтры могут быть реализованы как аппаратно, так и программно. В качестве пакетного фильтра могут быть использованы как обычный маршрутизатор, так и работающая на сервере программа, сконфигурированные таким образом, чтобы фильтровать входящие и исходящие пакеты.

Обладая рядом положительных качеств, пакетные фильтры не лишены серьезных недостатков. Они не обеспечивают высокой степени безопасности, так как проверяют только заголовки пакетов и не поддерживают многих необходимых функций защиты, например, аутентификацию конечных узлов, криптографическое закрытие пакетов сообщений, а также проверку их целостности и подлинности. Пакетные фильтры уязвимы для таких распространенных сетевых атак, как подмена исходных адресов и несанкционированное изменение содержимого пакетов сообщений. Однако такие достоинства пакетных фильтров, как простота реализации, высокая производительность, прозрачность для программных приложений и малая цена, обусловленная тем, что любой маршрутизатор в той или иной степени предоставляет возможность фильтрации пакетов, перевешивают указанные недостатки и обусловливают их повсеместное распространение и использование как обязательного элемента системы сетевой безопасности. Кроме того, они являются составной частью практически всех межсетевых экранов, использующих контроль состояния.

## 1.2 Шлюз сеансового уровня

Шлюз сеансового уровня, называемый еще экранирующим транспортом, предназначен для контроля виртуальных соединений и трансляции IР-адресов при взаимодействии с внешней сетью. Он функционирует на сеансовом уровне модели OSI, охватывая в процессе своей работы также транспортный и сетевой уровни эталонной модели. Защитные функции шлюза сеансового уровня относятся к функциям посредничества.

Контроль виртуальных соединений заключается в контроле квитирования связи, а также передачи информации по установленным виртуальным каналам. При контроле квитирования связи шлюз сеансового уровня следит за установлением виртуального соединения между рабочей станцией внутренней сети и компьютером внешней сети, определяя, является ли запрашиваемый сеанс связи допустимым.

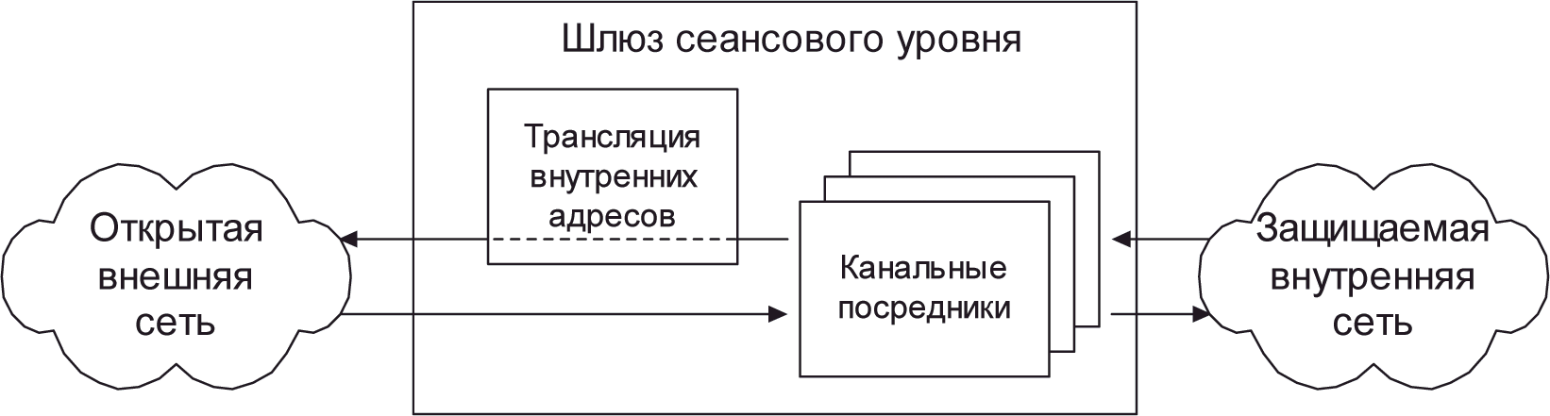
Такой контроль основывается на информации, содержащейся в заголовках пакетов сеансового уровня протокола ТСР. Однако если пакетный фильтр при анализе ТСР-заголовков проверяет только номера портов источника и получателя, то экранирующий транспорт анализирует другие поля, относящиеся к процессу квитирования связи.

Чтобы определить, является ли запрос на сеанс связи допустимым, шлюз сеансового уровня выполняет следующие действия. Когда рабочая станция (клиент) запрашивает связь с внешней сетью, шлюз принимает этот запрос, проверяя, удовлетворяет ли он базовым критериям фильтрации, например, может ли сервер определить IP-адрес клиента и ассоциированное с ним имя. Затем, действуя от имени клиента, шлюз устанавливает соединение с компьютером внешней сети и следит за выполнением процедуры квитирования связи по протоколу ТСР.

После того как шлюз определил, что рабочая станция внутренней сети и компьютер внешней сети являются авторизованными участниками сеанса ТСР, и проверил допустимость данного сеанса, он устанавливает соединение.

Начиная с этого момента шлюз копирует и перенаправляет пакеты туда и обратно, контролируя передачу информации по установленному виртуальному каналу.

Для контроля виртуальных соединений в шлюзах сеансового уровня используются специальные программы, которые называют канальными посредниками (Pipe Proxies). Эти посредники устанавливают между внутренней и внешней сетями виртуальные каналы, а затем контролируют передачу по этим каналам пакетов, генерируемых приложениями ТСР/№ (рис. 3).

Канальные посредники ориентированы на конкретные службы ТСР/IP. Поэтому шлюзы сеансового уровня могут использоваться для расширения возможностей шлюзов прикладного уровня, работа которых основывается на программах - посредниках конкретных приложений

***Рис. 3. Схема функционирования шлюза сеансового уровня***

Шлюз сеансового уровня обеспечивает также трансляцию внутренних адресов сетевого уровня (IP-адресов) при взаимодействии с внешней сетью. Трансляция внутренних адресов выполняется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов IP-адреса компьютеров-отправителей внутренней сети автоматически преобразуются в один IP-адрес, ассоциируемый с экранирующим транспортом. В результате все пакеты, исходящие из внутренней сети, оказываются отправленными межсетевым экраном, что исключает прямой контакт между внутренней и внешней сетями. IP-адрес шлюза сеансового уровня становится единственным активным IP-адресом, который попадает во внешнюю сеть.

Трансляция адресов вызвана необходимостью усиления защиты путем сокрытия от внешних пользователей структуры защищаемой внутренней сети. При трансляции внутренних IP-адресов шлюз сеансового уровня экранирует, то есть заслоняет, внутреннюю сеть от внешнего мира.

С другой стороны, трансляция адресов вызвана тем, что канальные посредники создают новое соединение каждый раз, когда они активируются. Посредник принимает запрос от рабочей станции внутренней сети и затем инициирует новый запрос к компьютеру внешней сети. Поэтому компьютер внешней сети воспринимает запрос как исходящий от посредника, а не от действительного клиента.

С точки зрения реализации шлюз сеансового уровня представляет собой довольно простую и относительно надежную программу. Он дополняет экранирующий маршрутизатор функциями контроля виртуальных соединений и трансляции внутренних 1Р-адресов.

Недостатки у шлюза сеансового уровня те же, что и у экранирующего маршрутизатора, - не обеспечиваются контроль и защита содержимого пакетов сообщений, не поддерживается аутентификация пользователей и конечных узлов, а также другие функции защиты локальной сети. У данной технологии есть еще один серьезный недостаток - невозможность проверки содержимого поля данных. В результате злоумышленнику предоставляется возможность передачи в защищаемую сеть троянских коней и других вредоносных программ.

На практике большинство шлюзов сеансового уровня не являются самостоятельными продуктами, а поставляются в комплекте со шлюзами прикладного уровня.

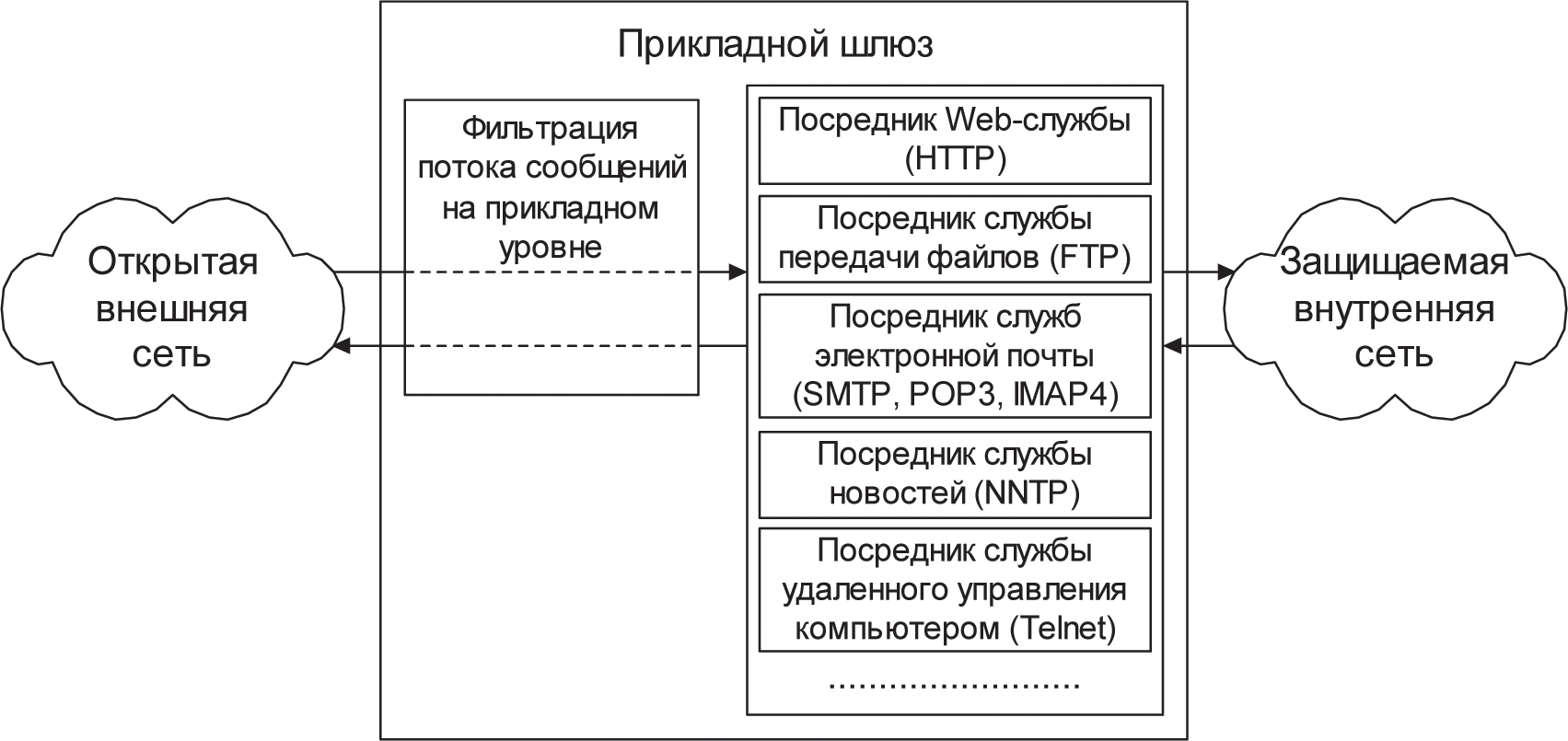
## 1.3.Прикладной шлюз

Прикладной шлюз, называемый также экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывая также уровень представления, и обеспечивает надежную защиту межсетевых взаимодействий. Защитные функции прикладного шлюза, как и шлюза сеансового уровня, относятся к функциям посредничества. Однако прикладной шлюз, в отличие от шлюза сеансового уровня, может выполнять существенно большее количество функций защиты, к которым относятся следующие:

* идентификация и аутентификация пользователей при попытке установления соединений через МЭ;
* проверка подлинности информации, передаваемой через шлюз;
* разграничение доступа к ресурсам внутренней и внешней сетей;
* фильтрация и преобразование потока сообщений, например, динамический поиск вирусов и прозрачное шифрование информации;
* регистрация событий, реагирование на задаваемые события, а также анализ зарегистрированной информации и генерация отчетов;
* кэширование данных, запрашиваемых из внешней сети.

Поскольку функции прикладного шлюза относятся к функциям посредничества, этот шлюз представляет собой универсальный компьютер, на котором функционируют программные посредники (экранирующие агенты) - по одному для каждого обслуживаемого прикладного протокола (HTTP, FTP, SMTP, NNTP и др.). Программный посредник (Application Рrоxу) каждой службы TCP/IP ориентирован на обработку сообщений и выполнение функций защиты, относящихся именно к этой службе.

Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, то есть прикладной шлюз функционирует в качестве сервера-посредника, исключая прямые соединения между внутренней и внешней сетями (рис. 4).

*Рис. 4. Схема функционирования прикладного шлюза *

Посредники, используемые прикладным шлюзом, имеют важные отличия от канальных посредников шлюзов сеансового уровня.

Во-первых, посредники прикладного шлюза связаны с конкретными приложениями (программными серверами), во-вторых, они могут фильтровать поток сообщений на прикладном уровне модели ОSI.

Прикладные шлюзы используют в качестве посредников специально разработанные для этой цели программные серверы конкретных служб ТСР/IР – серверы НТТР, FТР, SМТР, NNТР и др. Эти программные серверы функционируют на МЭ в резидентном режиме и реализуют функции защиты, относящиеся к соответствующим службам ТСР/IР. Трафик UDР обслуживается специальным транслятором содержимого UDР-пакетов.

Как и в случае шлюза сеансового уровня, для связи между рабочей станцией внутренней сети и компьютером внешней сети соответствующий посредник прикладного шлюза образует два соединения: от рабочей станции до МЭ и от МЭ до места назначения. Посредники прикладного шлюза пропускают только пакеты, сгенерированные теми приложениями, которые им поручено обслуживать. Например, программа -посредник службы НТТР может обрабатывать лишь трафик, генерируемый этой службой.

Если для какого-либо из приложений отсутствует свой посредник приложений, то прикладной шлюз не сможет обрабатывать трафик такого приложения, и он будет блокирован. Например, если прикладной шлюз использует только программы-посредники НТТР, FТР и Теlnet то он будет обрабатывать лишь пакеты, относящиеся к этим службам, блокируя при этом пакеты всех остальных служб.

Фильтрация потоков сообщений реализуется прикладными шлюзами на прикладном уровне модели OSI. Соответственно, посредники прикладного шлюза, в отличие от канальных посредников, обеспечивают проверку содержимого обрабатываемых пакетов. Они могут фильтровать отдельные виды команд или информации в сообщениях протоколов прикладного уровня, которые им поручено обслуживать. Например, для службы FTP возможно динамическое обезвреживание компьютерных вирусов в копируемых из внешней сети файлах. Кроме того, посредник данной службы может быть сконфигурирован таким образом, чтобы предотвращать использование клиентами команды PUT, предназначенной для записи файлов на FTP-сервер. Такое ограничение уменьшает риск случайного повреждения хранящейся на FTP-сервере информации и снижает вероятность переполнения его ненужными данными.

При настройке прикладного шлюза и описании правил фильтрации сообщений используются такие параметры, как название сервиса; допустимый временной интервал его использования; ограничения на содержимое сообщений, связанных с данным сервисом; компьютеры, с которых можно пользоваться сервисом; идентификаторы пользователей; схемы аутентификации и др.

Шлюз прикладного уровня обладает следующими достоинствами:

* обеспечивает высокий уровень защиты локальной сети благодаря возможности выполнения большинства функций посредничества;
* защита на уровне приложений позволяет осуществлять большое количество дополнительных проверок, уменьшая тем самым вероятность проведения успешных атак, основанных на недостатках программного обеспечения;
* при нарушении работоспособности прикладного шлюза блокируется сквозное прохождение пакетов между разделяемыми сетями, в результате безопасность защищаемой сети не снижается из-за возникновения отказов.

К недостаткам прикладного шлюза относятся:

* относительно высокая стоимость;
* довольно большая сложность самого МЭ, а также процедур его установки и конфигурирования;
* высокие требования к производительности и ресурсоемкости компьютерной платформы;
* отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

## 1.4.Шлюз экспертного уровня

Для устранения такого существенного недостатка прикладных шлюзов, как отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий, компания Check Рoint разработала технологию фильтрации пакетов, которую иногда называют фильтрацией с контролем состояния соединения (Stateful Inspection), или фильтрацией экспертного уровня. Такая фильтрация осуществляется на основе специальных методов многоуровневого анализа состояния пакетов SMLT (Stateful Мulti-Layer Technique).

Эта гибридная технология позволяет отслеживать состояние сетевого соединения, перехватывая пакеты на сетевом уровне и извлекая из них информацию прикладного уровня, которая используется для контроля за соединением. Быстрое сравнение проходящих пакетов с известным состоянием (State) «дружественных» пакетов позволяет значительно сократить время обработки, по сравнению с МЭ уровня приложений.

Межсетевые экраны, в основу функционирования которых положена описанная технология фильтрации, называют МЭ экспертного уровня. Такие МЭ сочетают в себе элементы экранирующих маршрутизаторов и прикладных шлюзов. Как и экранирующие маршрутизаторы, они обеспечивают фильтрацию пакетов по содержимому их заголовков сетевого и транспортного уровней модели QSI. МЭ экспертного уровня также выполняют все функции прикладного шлюза, касающиеся фильтрации пакетов на прикладном уровне модели QSI. Они оценивают содержимое каждого пакета в соответствии с заданной политикой безопасности.

Таким образом, МЭ экспертного уровня позволяют контролировать:

* каждый передаваемый пакет - на основе имеющейся таблицы правил;
* каждую сессию - на основе таблицы состояний;
* каждое приложение - на основе разработанных посредников.

Достоинством межсетевых экранов экспертного уровня является прозрачность для конечного пользователя, не требующая дополнительной настройки или изменения конфигурации клиентского программного обеспечения. Помимо прозрачности для пользователей и более высокой скорости обработки информационных потоков, к достоинствам межсетевых экранов экспертного уровня относится также то, что эти МЭ не изменяют IP-адресов, проходящих через них пакетов. Это означает, что любой протокол прикладного уровня, использующий IP-адреса, будет корректно работать с этими МЭ без каких-либо изменений или специального программирования.

Поскольку данные МЭ допускают прямое соединение между авторизованным клиентом и компьютером внешней сети, они обеспечивают менее высокий уровень защиты. Поэтому на практике технология фильтрации экспертного уровня используется для повышения эффективности функционирования комплексных МЭ.

## 1.5.Варианты исполнения межсетевых экранов

Существуют два основных варианта исполнения межсетевых экранов - программный и программно-аппаратный. В свою очередь, программно-аппаратный вариант исполнения межсетевых экранов имеет две разновидности - в виде специализированного устройства и в виде модуля в маршрутизаторе или коммутаторе.

В настоящее время чаще используется программное решение, которое на первый взгляд выглядит более привлекательным. Это связано с тем, что для его применения достаточно, казалось бы, только приобрести программное обеспечение межсетевого экрана и установить его на любой компьютер, имеющийся в организации. Однако на практике далеко не всегда в организации находится свободный компьютер, да еще и удовлетворяющий достаточно высоким требованиям по системным ресурсам.

Программно-аппаратный комплекс межсетевого экранирования обычно состоит из компьютера, а также функционирующих на нем операционной системы (ОС) и специального программного обеспечения. Следует отметить, что это специальное программное обеспечение часто называют firewall. Используемый компьютер должен быть достаточно мощным и физически защищенным, например, находиться в специально отведенном и охраняемом помещении. Кроме того, он должен иметь средства защиты от загрузки ОС с несанкционированного носителя. Программно-аппаратные комплексы используют специализированные или обычные операционные системы (как правило, на базе FгееВSD или Linuх), урезанные для выполнения заданных функций и удовлетворяющие ряду требований:

* иметь средства разграничения доступа к ресурсам системы;
* блокировать доступ к компьютерным ресурсам в обход предоставляемого программного интерфейса;
* запрещать привилегированный доступ к своим ресурсам из локальной сети;
* содержать средства мониторинга/аудита любых административных действий.

Специализированные программно-аппаратные решения обладают следующими достоинствами:

* простотой внедрения в технологию обработки информации. Такие средства поставляются уже с заранее установленной и настроенной операционной системой, и защитными механизмами, поэтому необходимо только подключить их к сети, что выполняется в течение нескольких минут;
* простотой управления. Данные средства могут управляться с любой рабочей станции Windows или UNIX. Взаимодействие консоли управления с устройством осуществляется либо по стандартным протоколам, например Теlnet или SNМР, либо при помощи специализированных или защищенных протоколов, например SSH или SSL;
* отказоустойчивостью и высокой доступностью. Исполнение межсетевого экрана в виде специализированного программно-аппаратного комплекса позволяет реализовать механизмы обеспечения не только программной, но и аппаратной отказоустойчивости и высокой доступности;
* высокой производительностью и надежностью. За счет исключения из операционной системы всех ненужных сервисов и подсистем программно-аппаратный комплекс работает более эффективно, с точки зрения производительности и надежности;
* специализацией на защите. Решение только задач обеспечения сетевой безопасности не приводит к затратам ресурсов на выполнение других функций, например, маршрутизации и т. п.

# 2.Схемы сетевой защиты на базе межсетевых экранов

При подключении корпоративной или локальной сети к глобальным сетям необходимо решать следующие задачи:

* защита корпоративной или локальной сети от несанкционированного удаленного доступа со стороны глобальной сети;
* сокрытие информации о структуре сети и ее компонентов от пользователей глобальной сети;
* разграничение доступа в защищаемую сеть из глобальной сети и из защищаемой сети в глобальную сеть.

Для эффективной защиты межсетевого взаимодействия система МЭ должна быть правильно установлена и сконфигурирована. Данный процесс состоит из следующих шагов:

* формирование политики межсетевого взаимодействия;
* выбор схемы подключения и настройка параметров функционирования межсетевого экрана.

## 2.1.Формирование политики межсетевого взаимодействия

Политика межсетевого взаимодействия является составной частью общей политики безопасности в организации. Политика межсетевого взаимодействия определяет требования к безопасности информационного обмена организации с внешним миром. Эта политика должна отражать два аспекта:

* политику доступа к сетевым сервисам;
* политику работы межсетевого экрана.

Политика доступа к сетевым сервисам определяет правила предоставления, а также использования всех возможных сервисов защищаемой компьютерной сети. В рамках данной политики должны быть заданы все сервисы, предоставляемые через межсетевой экран, и допустимые адреса клиентов для каждого сервиса. Кроме того, для пользователей должны быть указаны правила, описывающие, когда и какие пользователи каким сервисом и на каком компьютере могут воспользоваться.

Для того чтобы межсетевой экран успешно защищал ресурсы организации, политика доступа пользователей к сетевым сервисам должна быть реалистичной. Реалистичной считается такая политика, при которой найден баланс между защитой сети организации от известных рисков и необходимым доступом пользователей к сетевым сервисам.

Политика работы межсетевого экрана задает базовый принцип управления межсетевым взаимодействием, положенный в основу функционирования МЭ. Может быть выбран один из двух таких принципов:

* запрещено все, что явно не разрешено;
* разрешено все, что явно не запрещено.

Фактически выбор принципа устанавливает, насколько «подозрительной» или «доверительной» должна быть система защиты. В зависимости от выбора решение может быть принято, как в пользу безопасности в ущерб удобству использования сетевых сервисов, так и наоборот.

При выборе принципа «запрещено все, что явно не разрешено» межсетевой экран настраивается таким образом, чтобы блокировать любые явно неразрешенные межсетевые взаимодействия. Данный принцип соответствует классической модели доступа, используемой во всех областях информационной безопасности. Такой подход позволяет адекватно реализовать принцип минимизации привилегий, поэтому с точки зрения безопасности он является лучшим. Администратор безопасности должен на каждый тип разрешенного взаимодействия задавать одно и более правил доступа. Администратор не сможет по забывчивости оставить разрешенными какие-либо полномочия, так как по умолчанию они будут запрещены. Доступные лишние сервисы могут быть использованы во вред безопасности, что особенно характерно для закрытого и сложного программного обеспечения, в котором могут быть различные ошибки и некорректности. Принцип «запрещено все, что явно не разрешено», в сущности, является признанием факта, что незнание может причинить вред. Следует отметить, что правила доступа, сформулированные в соответствии с этим принципом, могут доставлять пользователям определенные неудобства.

При выборе принципа «разрешено все, что явно не запрещено» межсетевой экран настраивается таким образом, чтобы блокировать только явно запрещенные межсетевые взаимодействия. В этом случае повышается удобство использования сетевых сервисов со стороны пользователей, но снижается безопасность межсетевого взаимодействия. Пользователи имеют больше возможностей обойти межсетевой экран, например, могут получить доступ к новым сервисам, не запрещаемым политикой (или даже не указанным в политике), или запустить неразрешенные сервисы на нестандартных портах TCP/ UDP, которые не запрещены политикой. Администратор может учесть не все действия, которые запрещены пользователям. Ему приходится работать в режиме реагирования, предсказывая и запрещая те межсетевые взаимодействия, которые отрицательно воздействуют на безопасность сети. При реализации данного принципа внутренняя сеть оказывается менее защищенной от нападений хакеров. Поэтому производители межсетевых экранов обычно отказываются от использования данного принципа.

Межсетевой экран не является симметричным. Для него отдельно задаются правила, ограничивающие доступ из внутренней сети во внешнюю сеть и наоборот. В общем случае работа межсетевого экрана основана на динамическом выполнении двух групп функций:

* фильтрации проходящих через него информационных потоков;
* посредничества при реализации межсетевых взаимодействий.

В зависимости от типа экрана эти функции могут выполняться с различной полнотой. Простые межсетевые экраны ориентированы на выполнение только одной из данных функций. Комплексные МЭ обеспечивают совместное выполнение указанных функций защиты. Собственная защищенность межсетевого экрана достигается с помощью тех же средств, что и защищенность универсальных систем.

Чтобы эффективно обеспечивать безопасность сети, комплексный МЭ обязан управлять всем потоком, проходящим через него, и отслеживать свое состояние. Для принятия управляющих решений по используемым сервисам МЭ должен получать, запоминать, выбирать и обрабатывать информацию, полученную от всех коммуникационных уровней и от других приложений.

Недостаточно просто проверять пакеты по отдельности. Информация о состоянии соединения, полученная из инспекции соединений в прошлом и других приложений, - главный фактор в принятии управляющего решения при попытке установления нового соединения. Для принятия решения могут учитываться как состояние соединения (полученное из прошлого потока данных), так и состояние приложения (полученное из других приложений). Полнота и правильность управления требуют, чтобы комплексный МЭ имел возможность анализа и использования следующих элементов:

* информации о соединениях - информации от всех семи уровней в пакете;
* истории соединений - информации, полученной от предыдущих соединений;
* состояния уровня приложения - информации о состоянии, полученной из других приложений. Например, аутентифицированному до настоящего момента пользователю можно предоставить доступ через МЭ только для авторизованных видов сервиса;
* агрегирующих элементов - вычислений разнообразных выражений, основанных на всех вышеперечисленных факторах.

## 2.2.Основные схемы подключения межсетевых экранов

При подключении корпоративной сети к глобальным сетям необходимо разграничить доступ в защищаемую сеть из глобальной и из защищаемой сети в глобальную, а также обеспечить защиту подключаемой сети от несанкционированного удаленного доступа со стороны глобальной сети. При этом организация заинтересована в сокрытии информации о структуре своей сети и ее компонентов от пользователей глобальной сети. Работа с удаленными пользователями требует установления жестких ограничений доступа к информационным ресурсам защищаемой сети.

У организации часто возникает потребность иметь в составе корпоративной сети несколько сегментов с разными уровнями защищенности:

* свободно доступные сегменты (например, рекламный WWW- сервер);
* сегмент с ограниченным доступом (например, для доступа сотрудникам организации с удаленных узлов);
* закрытые сегменты (например, финансовая локальная подсеть организации).

Для подключения межсетевых экранов могут использоваться различные схемы, которые зависят от условий функционирования защищаемой сети, а также от количества сетевых интерфейсов и других характеристик, используемых МЭ. Широкое распространение получили следующие схемы подключения межсетевых экранов:

* схемы защиты сети с использованием экранирующего маршрутизатора;
* схемы единой защиты локальной сети;
* схемы с защищаемой закрытой и незащищаемой открытой подсетями;
* схемы с раздельной защитой, закрытой и открытой подсетей.

Схема защиты с использованием экранирующего маршрутизатора. Межсетевой экран, основанный на фильтрации пакетов, является самым распространенным и наиболее простым в реализации. Он состоит из экранирующего маршрутизатора, расположенного между защищаемой сетью и потенциально враждебной открытой внешней сетью (рис. 5). Экранирующий маршрутизатор (пакетный фильтр) сконфигурирован для блокирования или фильтрации входящих и исходящих пакетов на основе анализа их адресов и портов.

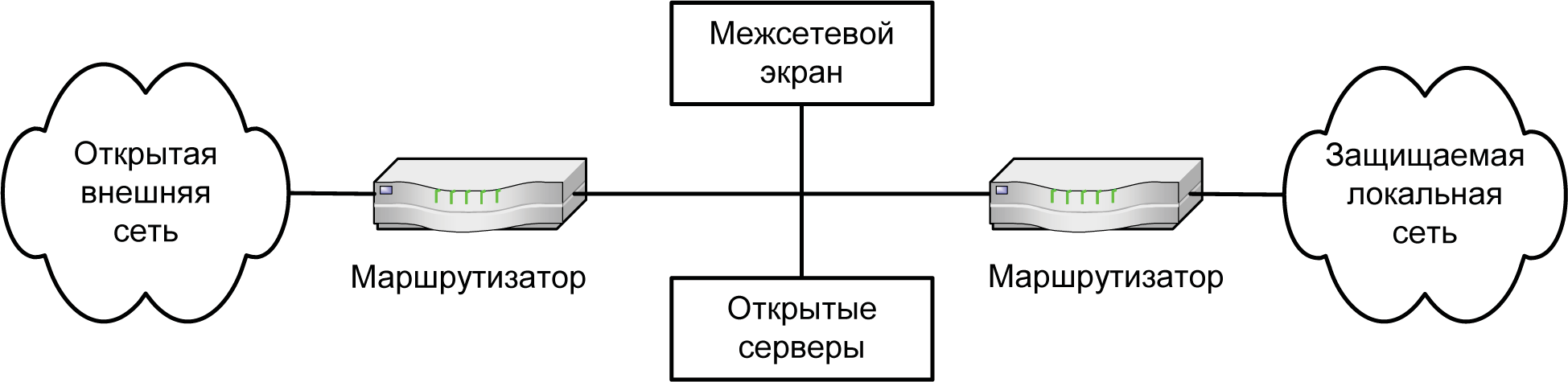
**Рис. 5. Межсетевой экран - экранирующий маршрутизатор**

Компьютеры, находящиеся в защищаемой сети, имеют прямой доступ в сеть Интернет, в то время как большая часть доступа к ним из Интернета блокируется. В принципе, экранирующий маршрутизатор может реализовать любую из политик безопасности, описанных ранее. Однако если маршрутизатор не фильтрует пакеты по порту источника и номеру входного и выходного порта, то реализация политики «запрещено все, что не разрешено в явной форме» может быть затруднена.

Межсетевые экраны, основанные на фильтрации пакетов, имеют те же недостатки, что и экранирующие маршрутизаторы, причем эти недостатки становятся более ощутимыми при ужесточении требований к безопасности защищаемой сети. Отметим некоторые из них:

* сложность правил фильтрации, в некоторых случаях совокупность этих правил может стать неуправляемой;
* невозможность полного тестирования правил фильтрации, это приводит к незащищенности сети от непротестированных атак;
* О практически отсутствующие возможности регистрации событий, в результате администратору трудно определить, подвергался ли маршрутизатор атаке и скомпрометирован ли он.

Схемы подключения межсетевых экранов с несколькими сетевыми интерфейсами. Схемы защиты с МЭ с одним сетевым интерфейсом (рис. 6) недостаточно эффективны как с точки зрения безопасности, так и с позиций удобства конфигурирования.



*Рис. 6. Защита локальной сети c помощью МЭ с одним сетевым интерфейсом*

Они физически не разграничивают внутреннюю и внешнюю сети и, соответственно, не могут обеспечивать надежную защиту межсетевых взаимодействий. Настройка таких межсетевых экранов, а также связанных с ними маршрутизаторов представляет собой довольно сложную задачу, цена решения которой превышает стоимость замены МЭ с одним сетевым интерфейсом на МЭ с двумя или тремя сетевыми интерфейсами. Поэтому далее будут более подробно рассмотрены схемы подключения межсетевых экранов с двумя и тремя сетевыми интерфейсами.

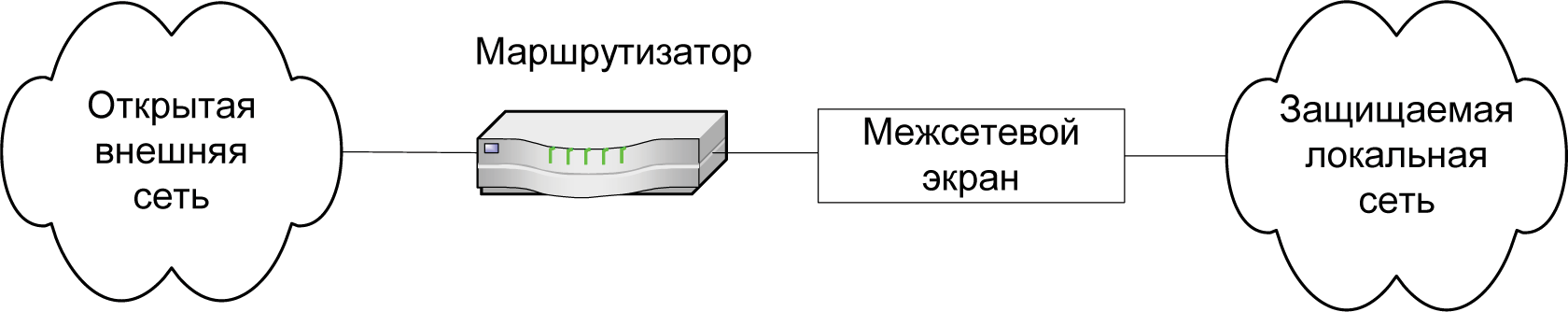
Защищаемую локальную сеть целесообразно представлять, как совокупность закрытой и открытой подсетей. Здесь под открытой подсетью понимается подсеть, доступ к которой со стороны потенциально враждебной внешней сети может быть полностью или частично открыт. В открытую подсеть могут, например, входить общедоступные WWW-, FТР- и SМТР-серверы, а также терминальный сервер с модемным пулом.

Среди множества возможных схем подключения МЭ типовыми являются следующие:

* схема единой защиты локальной сети;
* схема с защищаемой закрытой и незащищаемой открытой подсетями;
* схема с раздельной защитой закрытой и открытой подсетей.

Схема единой защиты локальной сети. Данная схема является наиболее простым решением (рис. 7), при котором МЭ целиком экранирует локальную сеть от потенциально враждебной внешней сети. Между маршрутизатором и МЭ имеется только один путь, по которому идет весь трафик. Данный вариант МЭ реализует политику безопасности, основанную на принципе «запрещено все, что явно не разрешено»; при этом пользователю недоступны все службы, кроме

тех, для которых определены соответствующие полномочия. Обычно маршрутизатор настраивается таким образом, что МЭ является единственным видимым снаружи сетевым устройством.

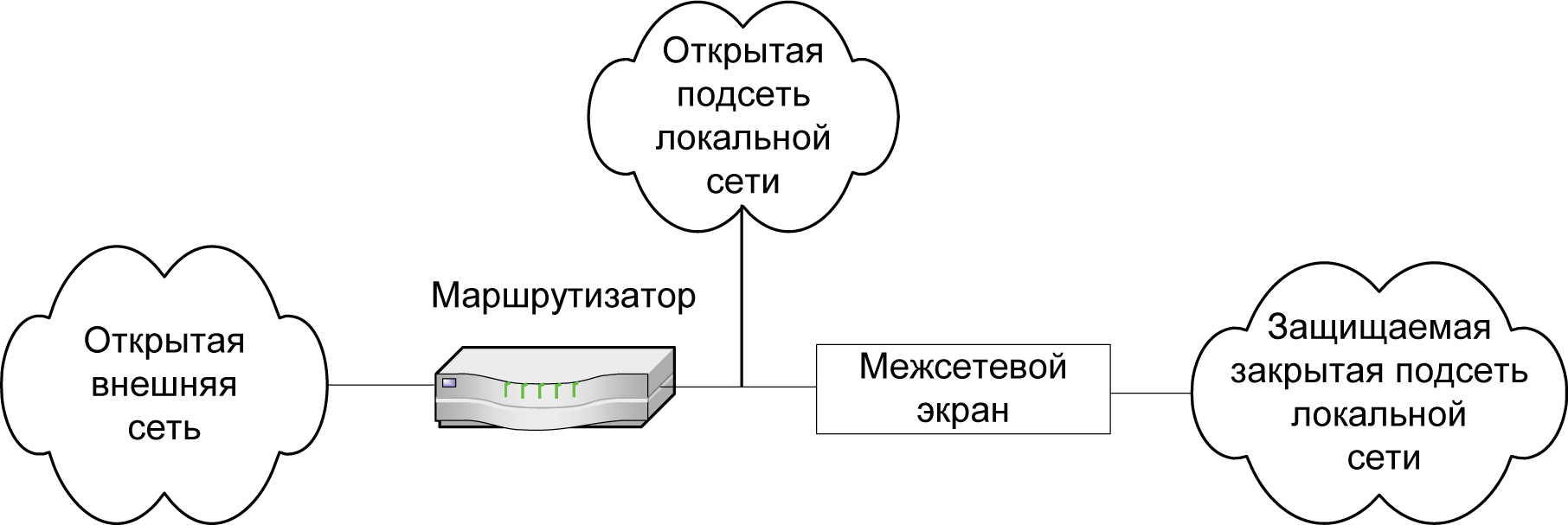


**Рис. 7. Схема единой защиты локальной сети**

Открытые серверы, входящие в локальную сеть, также будут защищены межсетевым экраном. Однако объединение серверов, доступных из внешней сети, вместе с другими ресурсами защищаемой локальной сети существенно снижает безопасность межсетевых взаимодействий. Поэтому данную схему подключения МЭ можно использовать лишь при отсутствии в локальной сети открытых серверов или, когда имеющиеся открытые серверы делаются доступными из внешней сети только для ограниченного числа пользователей, которым можно доверять.

Поскольку межсетевой экран использует хост, то на нем могут быть установлены программы для усиленной аутентификации пользователей. Межсетевой экран может также протоколировать доступ, попытки зондирования и атак системы, что позволит выявить действия злоумышленников.

Для некоторых сетей может оказаться неприемлемой недостаточная гибкость схемы защиты на базе межсетевого экрана с двумя интерфейсами.

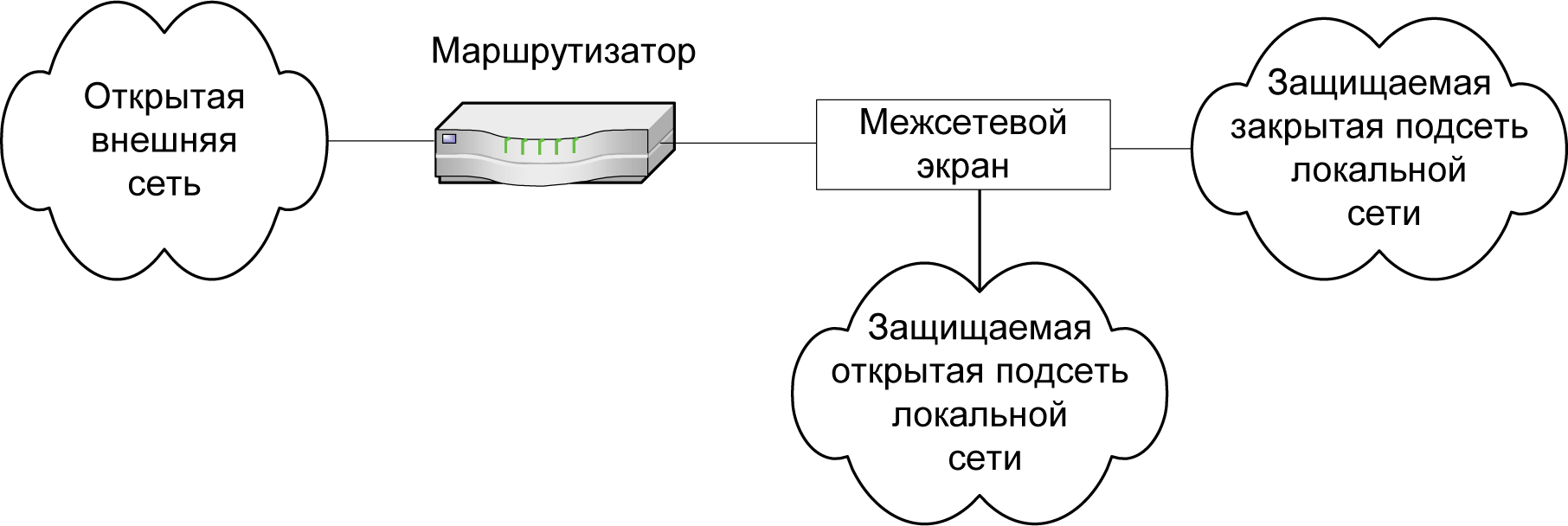
Схема с защищаемой закрытой и незащищаемой открытой подсетями. Если в составе локальной сети имеются общедоступные открытые серверы, тогда их целесообразно вынести как открытую подсеть до межсетевого экрана (рис. 8). Данный способ обладает более высокой защищенностью закрытой части локальной сети, но обеспечивает пониженную безопасность открытых серверов, расположенных до межсетевого экрана. Некоторые МЭ позволяют разместить эти серверы на себе. Однако такое решение не является лучшим с точки зрения безопасности самого МЭ и загрузки компьютера. Схему подключения МЭ с защищаемой закрытой подсетью и незащищаемой открытой подсетью целесообразно использовать лишь при невысоких требованиях по безопасности к открытой подсети.

***Рис. 8. Схема с защищаемой закрытой и незащищаемой открытой подсетями***

Если же к безопасности открытых серверов предъявляются повышенные требования, тогда необходимо использовать схему с раздельной защитой закрытой и открытой подсетей.

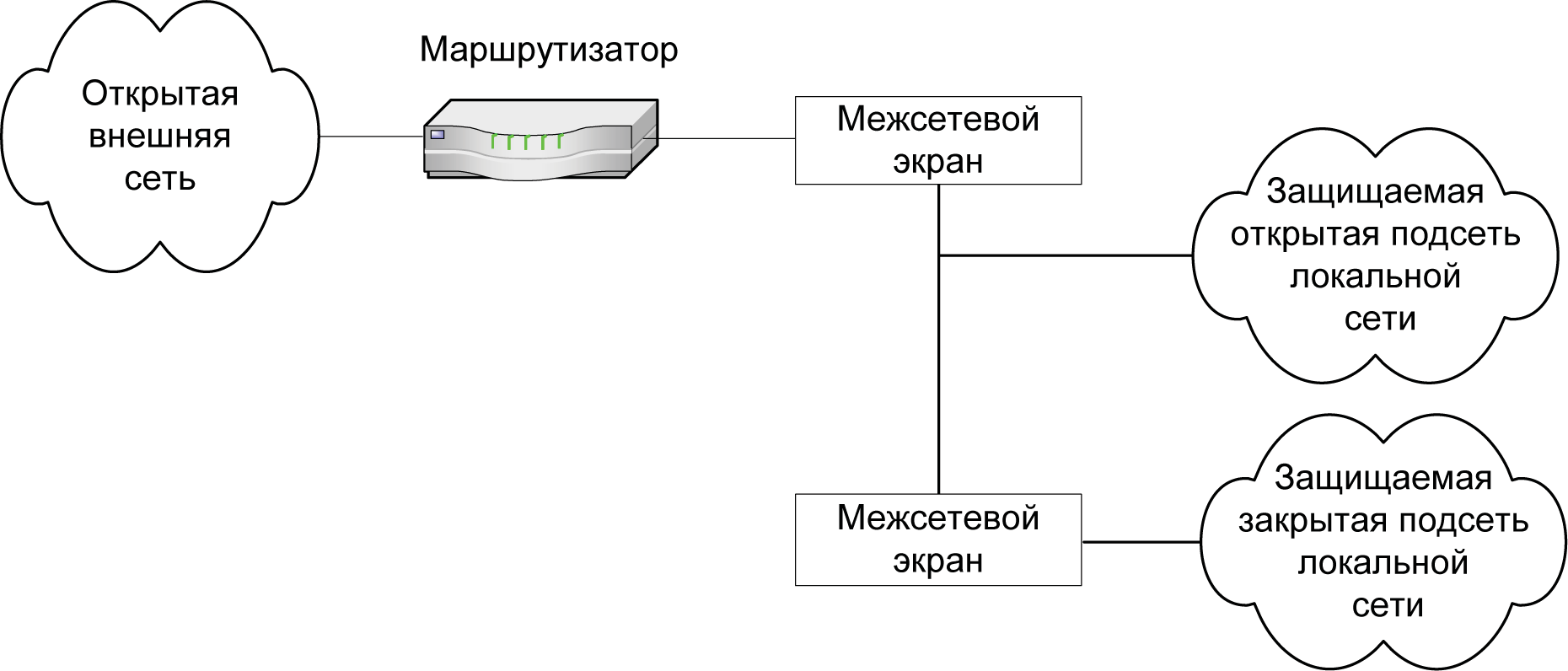
***Схемы с раздельной защитой закрытой и открытой подсетей.***

Такая схема может быть построена на основе одного МЭ с тремя сетевыми интерфейсами (рис. 9) или на основе двух МЭ с двумя сетевыми интерфейсами (рис. 10). В обоих случаях доступ к открытой и закрытой подсетям локальной сети возможен только через межсетевой экран. При этом доступ к открытой подсети не позволяет осуществить доступ к закрытой подсети.



***Рис. 9. Схема с раздельной защитой закрытой и открытой подсетей на основе одного МЭ с тремя сетевыми интерфейсами***

Из этих двух схем большую степень безопасности межсетевых взаимодействий обеспечивает схема с двумя МЭ, каждый из которых образует отдельный эшелон защиты закрытой подсети. Защищаемая открытая подсеть здесь выступает в качестве экранирующей подсети.



**Рис. 10. Схема с раздельной защитой закрытой и открытой подсетей на основе двух МЭ с двумя сетевыми интерфейсами**

Обычно экранирующую подсеть конфигурируют таким образом, чтобы обеспечить доступ к компьютерам подсети как из потенциально враждебной внешней сети, так и из закрытой подсети локальной сети. Однако прямой обмен информационными пакетами между внешней сетью и закрытой подсетью невозможен. При атаке системы с экранирующей подсетью необходимо преодолеть по крайней мере две независимые линии защиты, что является весьма сложной задачей. Средства мониторинга состояния межсетевых экранов позволяют практически всегда обнаружить подобную попытку, и администратор системы может своевременно предпринять необходимые действия по предотвращению несанкционированного доступа.

## 2.3.Персональные и распределенные сетевые экраны

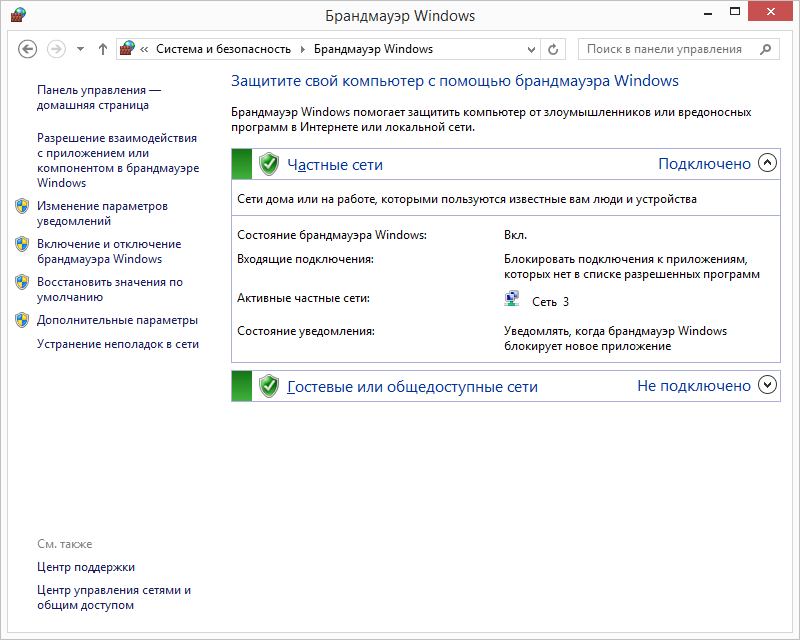
За последние несколько лет в структуре корпоративных сетей произошли определенные изменения. Если раньше границы таких сетей можно было четко очертить, то сейчас это практически невозможно. Еще недавно такая граница проходила через все маршрутизаторы или иные устройства, через которые осуществлялся выход во внешние сети. С появлением новых сервисов и технологий, в частности мобильного доступа к ЛВС или использования беспроводных сегментов сети, понятие «периметра» начинает терять свое значение.

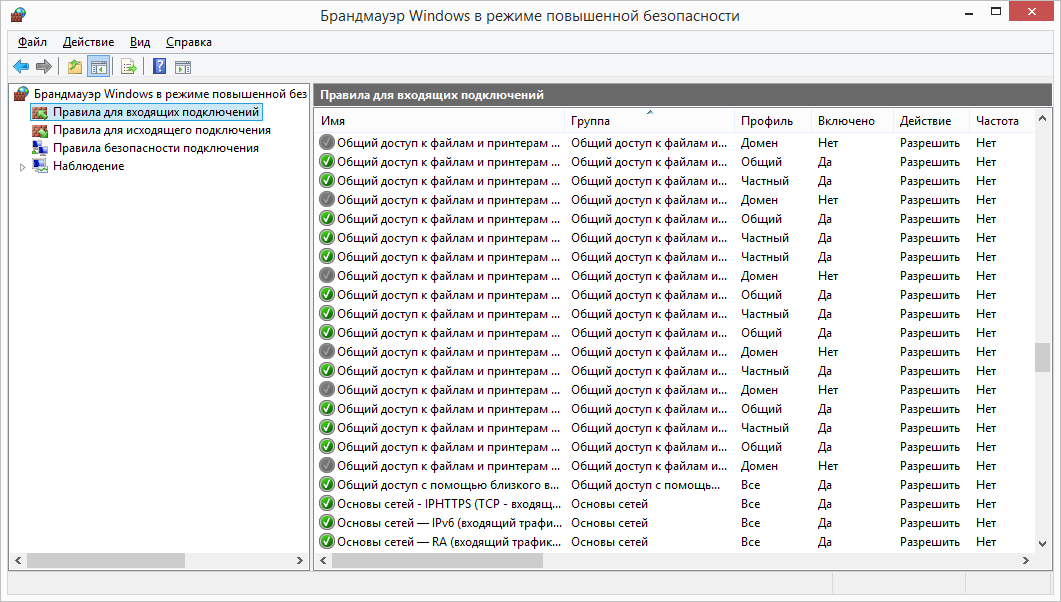
Наиболее уязвимым местом корпоративной сети являются рабочие станции конечных пользователей, находящиеся за пределами защищаемого периметра, которые имеют, как правило, низкий уровень защиты. Все традиционные межсетевые экраны построены так, что защищаемые пользователи и ресурсы должны находиться под их защитой с внутренней стороны корпоративной или локальной сети, что является невозможным для мобильных пользователей.

Следует также упомянуть о такой проблеме, как обеспечение внутренней безопасности сети. Технология обеспечения внутренней безопасности отличается от технологии защиты периметра. Для отражения атак из внешней по отношению к ЛВС сети существуют весьма эффективные средства, которые помогают защитить рабочие станции пользователей от атак и других подозрительных действий, направленных на получение конфиденциальной информации. А вот отследить и предотвратить атаки, организуемые из локальной сети, по-прежнему достаточно сложно. И опасности, связанные с внутренней безопасностью, постоянно растут.

Для решения указанных проблем предложены следующие подходы: применение персональных и распределенных межсетевых экранов и использование возможностей виртуальных частных сетей VPN.

Для индивидуальных пользователей представляет интерес технология персонального сетевого экранирования. В этом случае сетевой экран устанавливается на защищаемый персональный компьютер. Такой экран, называемый персональным экраном компьютера (Personal Firewall), или системой сетевого экранирования, контролирует весь исходящий и входящий трафик независимо от всех прочих системных защитных средств. При экранировании отдельного компьютера поддерживается доступность сетевых сервисов, но уменьшается нагрузка, индуцированная внешней активностью. В результате снижается уязвимость внутренних сервисов защищаемого таким образом компьютера, поскольку сторонний злоумышленник должен сначала преодолеть экран, где защитные средства сконфигурированы особенно тщательно и жестко. Для защиты рабочего места пользователя необходимо иметь, кроме персонального МЭ, антивирусное ПО с актуальными сигнатурами, защиту доступа в корпоративную сеть через VPN.

В качестве примера персонального сетевого экрана можно указать межсетевой экран Брандмауэр Windows, который служит первой линией защиты персонального компьютера от различного рода вредоносных программ.

***Рис. 11. Окно управления Брандмауэром Windows на примере Windows 8.1.***

***Рис. 12. Окно настроек правил Брандмауэра Windows на примере Windows 8.1***

При надлежащей настройке межсетевой экран Брандмауэр Windows не позволяет большинству вредоносных программ проникать в систему, обеспечивая защиту от хакеров, вирусов и компьютерных червей, которые пытаются получить доступ к компьютеру через Интернет.

Персонального сетевой экран может быть встроен в антивирусное ПО, например, компонента «Сетевой экран», входящая в состав продукта Kaspersky Endpoint Security.

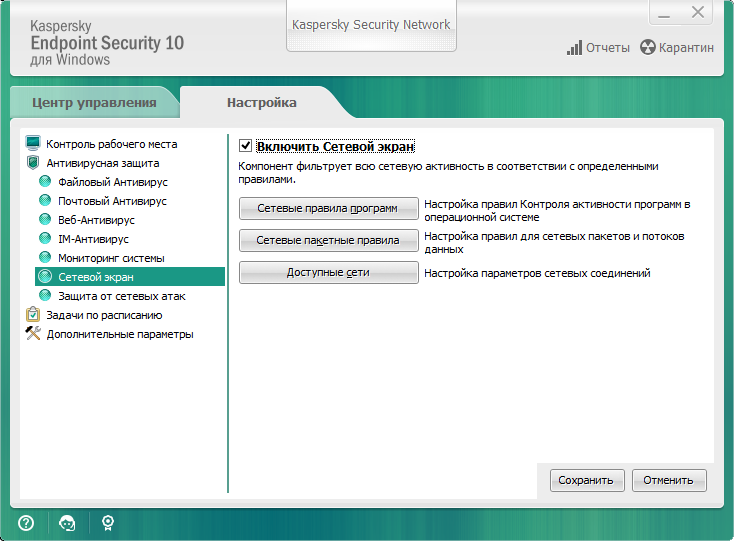
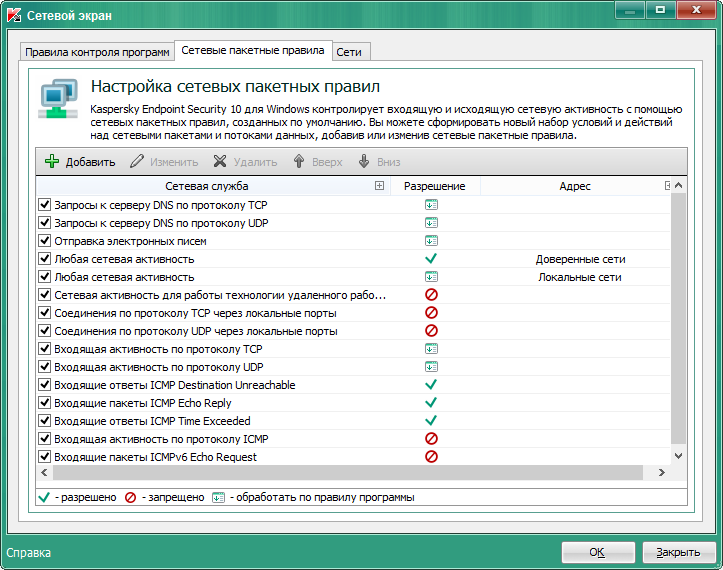
Рис 13. Окно управления настройками Сетевого экрана Kaspersky Endpoint Security 10.

Рис 14. Окно управления настройками сетевых пакетных правил Kaspersky Endpoint Security 10.

Распределенный межсетевой экран представляет собой централизованно управляемую совокупность сетевых мини-экранов, защищающих отдельные компьютеры сети. При построении распределенных систем МЭ их функциональные компоненты распределяются по узлам сети и могут обладать различной функциональностью. При обнаружении подозрительных на атаку признаков управляющие модули распределенного МЭ могут адаптивно изменять конфигурацию, состав и расположение компонентов.

Главное отличие распределенного межсетевого экрана от персонального экрана заключается в наличии у распределенного межсетевого экрана функции централизованного управления. Если персональные сетевые экраны управляются только с того компьютера, на котором они установлены, и идеально подходят для домашнего применения, то распределенные межсетевые экраны могут управляться централизованно, с единой консоли управления, установленной в главном офисе организации. Такие отличия позволили некоторым производителям выпускать свои решения МЭ в двух версиях:

* персональной (для индивидуальных пользователей);
* распределенной (для корпоративных пользователей).

В современных условиях более 60% различных атак и попыток доступа к информации осуществляются изнутри локальных сетей, поэтому классический «периметровый» подход к созданию системы защиты корпоративной сети становится недостаточно эффективным. Корпоративную сеть можно считать действительно защищенной от НСД только при наличии в ней как средств защиты точек входа со стороны Интернета, так и решений, обеспечивающих безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия. Решения на основе распределенных или персональных межсетевых экранов наилучшим образом обеспечивают безопасность отдельных компьютеров, корпоративных серверов и фрагментов локальной сети предприятия.