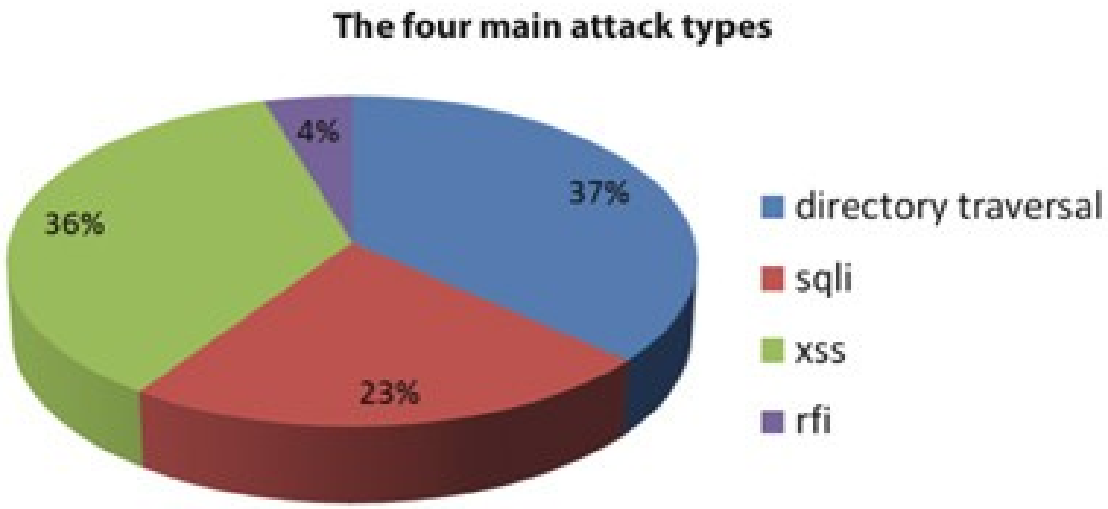
Практические примеры инцидентов **в информационно-телекоммуникационных сетях**
Рассмотрим ряд инцидентов, произошедших за последние годы и попавшие в ленты новостей:

- **Imperva проанализировала 10 миллионов атак на web-приложения (новость от 25 июля 2011, размещена на ресурсе www.securitylab.ru)**

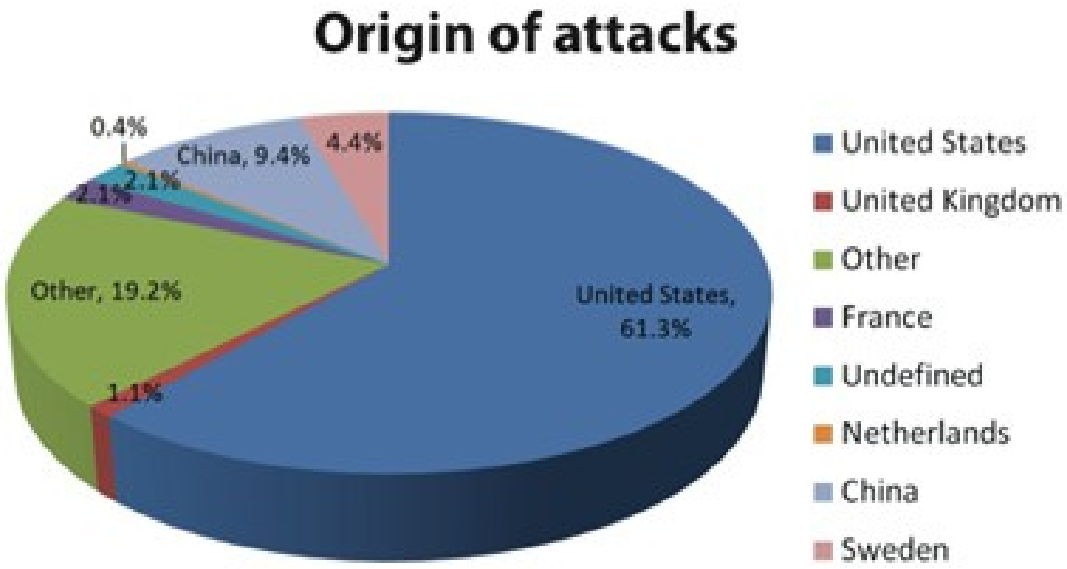
Веб-приложения в среднем подвергаются 27-ми вирусным атакам в час, или примерно 1-ой атаке каждые две минуты, согласно данным Imperva - компании, которая занимается разработкой и производством продуктов для защиты web-приложений и систем управления базами данных. Компания проанализировала 10 миллионов атак, нацеленных на web-приложения за 6 месяцев.
Проведенный анализ показывает, что когда web-сайты попадают под автоматизированную атаку, то в час проводится 25.000 специально сформированных запросов, или 7 – в секунду. Было выделено 4 основных типа атак, которые нацелены на веб-приложения: обход каталога (Directory Traversal), межсайтовое выполнение сценариев (Cross-Site Scripting), внедрение операторов SQL (SQL injection), и внедрение удаленного файла (Remote File Inclusion).



Современные ботнеты сканируют и исследуют всемирную сеть Интернет с целью использования уязвимостей и извлечения ценных данных, взлома паролей, распространения спама и вредоносного ПО, и манипуляции поисковыми механизмами.

Кроме того анализ показал, что автоматизированные атаки совершаются как на известные, так и на малоизвестные сайты, коммерческие и некоммерческие организации.

Более 61% исследованных атак совершались ботами из США. Атаки из Китая составили 10% от общего количества атак.



- **Суд в Германии признал DDoS-атаки уголовным преступлением (новость от 14 июня 2011, размещена на ресурсе www.lenta.ru)**

Суд в Германии признал блокирование интернет-сайтов путем преднамеренной перегрузки запросами уголовно наказуемым преступлением [Der Spiegel].

В соответствии с постановлением земельного суда Дюссельдорфа, организация DDoS-атаки на сервер будет караться лишением свободы на срок до десяти лет.

Это решение было принято судом в марте 2011 года. Поводом стало дело о блокировке работы

букмекерских сайтов. Обвиняемый, чье имя не называется, пытался шантажировать владельцев онлайн-контор, атаковав их сервера, расположенные в России.

Три компании из шести согласились откупиться от злоумышленника, оставшиеся три платить отказались. После этого обвиняемый вновь заблокировал их сайты. В результате они понесли убытки, общий объем которых исчисляется сотнями тысяч евро.

Подсудимого признали виновным не только в шантаже, но и в саботаже компьютерной техники (статья 303b Уголовного кодекса). Это дело стало одним из первых случаев вынесения обвинительного приговора в связи с организацией DDoS-атаки.

- **Полиция Гонконга арестовала хакера за взлом фондовой биржи (новость от 23 августа 2011, размещена на ресурсе www.securitylab.ru)**

Полицейские арестовали 29-летнего подозреваемого из округа Квун Тонг (Kwun Tong). В ходе ареста были изъяты компьютер подозреваемого, его сотовый телефон и цифровой RAID массив. Подозреваемый обвиняется в преднамеренном нанесении ущерба с использованием компьютерных технологий.
Фондовая биржа Гонконга была вынуждена приостановить торги в некоторых направлениях почти на две недели в связи с хакерскими атаками, которые вывели из строя сайт www.hkexnews.hk.
Недоступность сайта фондовой биржи сделала невозможным работу 8 компаний, включая HSBC, Cathay Pacific и Dah Sing Bank, которые должны были опубликовать результаты торгов.

- **Sony: 10 млн номеров кредитных карт оказались в руках хакеров (новость от 2 мая 2011, размещена на ресурсе www.securitylab.ru)**

Компания Sony предоставила новые данные, связанные со взломом сети Playstation Network и сервиса Qriocity. По сообщению компании, впервые доступ к платформе хакеры получили около двух недель назад, а всего в их руках оказались примерно 10 млн номеров карт.

За две недели до этого, злоумышленники вторглись на серверы Sony, расположенные в датацентре американского города Сан-Диего и технически они имели доступ к 77 млн учетных записей пользователей Playstation Network.

- **Жительница Канады требует от Sony миллиард долларов (новость от 5 мая 2011, размещена на ресурсе www.securitylab.ru)**

Жительница Канады подала иск против компании Sony, потребовав возместить ей миллиард канадских долларов (один миллиард 40 миллионов долларов США). Об этом сообщили представители юридической фирмы исца.

Иск был подан компанией McPhadden Samac Tuovi LLP из Торонто, которая представляет интересы 21-летней жительницы Онтарио Наташи Максимович. Она утверждает, что как многолетний пользователь сервиса PlayStation Network была поражена слабостью защиты Sony, которая привела к массовой утечке

конфиденциальных данных пользователей сети. Наташа хочет вложить деньги, которые она рассчитывает получить от Sony, в оплату мониторинга счетов потерпевших пользователей PSN для предотвращения мошенничества с ними в течение двух лет. В иске не уточняется, пойдут ли эти деньги на оплату мониторинга счетов всех пострадавших пользователей или же только проживающих в Канаде.

- **Утечка в бостонском аэропорте: инсайдер торговал персональными данными сотрудников (новость от 15 января 2010, размещена на ресурсе www.securitylab.ru)**

В бостонском аэропорте Logan обнаружили работника, который воровал, а затем продавал персональные данные своих сослуживцев. Им оказался сотрудник подразделения Администрации транспортной безопасности США (Transportation Security Administration, TSA).

Имя самого работника пока не разглашается. Однако известны имена сообщников. 46-летняя Тина Вайт (Tina M. White) и 48-летний Майкл Вашингтон (Michael J. Washington) получали персональные данные от племянницы Вашингтона, которая, собственно, и работала в отделе кадров аэропорта. Затем данные (имена, даты рождения и номера социального страхования) продавались по цене в $40 за одного человека.

Нашелся и один из пострадавших от кражи личности работников TSA. Лора Гигант (Laura Gigante) заявила, что масштабы махинаций впечатляющи. Используя ее персональные данные, мошенники регистрировали аккаунты в DirectTV, AT&T и NStar.

- **Киберпреступники наносят Великобритании ежегодный ущерб 27 млрд фунтов (новость от 18 февраля 2011, размещена на ресурсе www.securitylab.ru)**

Киберпреступность обходится британской экономике в 27 млрд фунтов ежегодно, сообщили в правительстве Британии.

Подобные данные были представлены впервые; их сбором занимались государственное Управление по киберпреступности и компания Detica, специализирующаяся на системах сетевой безопасности.

Этот отчет станет одним из основных документов при разработке правительством программы по борьбе с киберпреступностью, которую власти называют растущей угрозой.

В соответствии со статистическими данными, больше всего по вине кибермошенников теряет британский бизнес - 21 млрд фунтов; госструктуры лишаются 2,2 млрд фунтов, а частные лица – 3,1 млрд. Эти оценки не являются окончательными, в реальности масштаб потерь может быть гораздо больше.

Около половины из 21 млрд фунтов приходится на незаконное скачивание из сети материалов, являющихся интеллектуальной собственностью. Существенную проблему представляет также промышленный шпионаж.

Борьба с преступлениями в сфере высоких технологий осложняется тем, что многие пострадавшие от кибератак компании часто не признают этого факта, чтобы не испортить свою репутацию. Именно поэтому, во многом, сложно более точно оценить последствия такого рода преступлений для британской экономики.

Было заявлено, что на цели по борьбе с преступлениями в сфере высоких технологий в ближайшие четыре года будет израсходовано 650 млн фунтов.

Технологии межсетевых экранов.

- Функции межсетевых экранов, особенности функционирования межсетевых экранов на различных уровнях модели OSI.
- Критерии оценки качества межсетевых экранов: общие требования; основные классы защищенности межсетевых экранов в соответствии с руководящими документами ФСТЭК России.
- Обзор современных межсетевых экранов.
- Примеры работы межсетевых экранов для различных сценариев передачи информации.
-

Функции межсетевых экранов, особенности функционирования межсетевых экранов на различных уровнях модели OSI.

Межсетевой экран (МЭ) – это специализированный комплекс межсетевой защиты, называемый также брандмауэром или системой firewall. Межсетевой экран позволяет разделить общую сеть на две части или более и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую. Как правило, эта граница проводится между локальной сетью и глобальной сетью Интернет.

Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью.

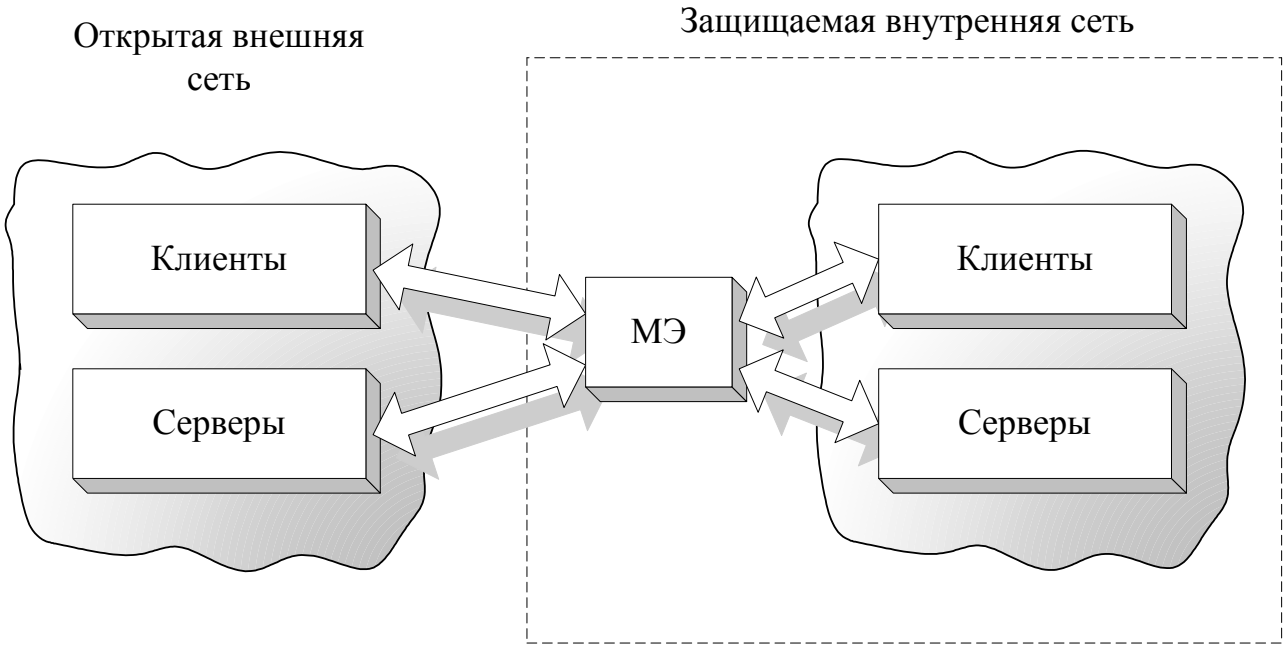


Рис.1. Схема подключения межсетевого экрана

При этом все взаимодействия между этими сетями должны осуществляться только через МЭ.

Межсетевой экран, защищающий сразу множество узлов внутренней сети, призван решить две основные задачи:

1) ограничение доступа внешних (по отношению к защищаемой сети) пользователей к внутренним ресурсам локальной сети;
2) разграничение доступа пользователей защищаемой сети к внешним ресурсам.

Межсетевые экраны можно классифицировать по следующим основным признакам:

1. По функционированию на уровнях модели OSI:
   - пакетный фильтр (экранирующий маршрутизатор – screening router);
   - шлюз сеансового уровня (экранирующий транспорт);
   - прикладной шлюз (application gateway);
   - шлюз экспертного уровня (stateful inspection firewall).
2. По используемой технологии:
   - контроль состояния протокола (stateful inspection);
   - на основе модулей посредников (proxy).
3. По исполнению:
   - программно–аппаратный;
   - программный.
4. По схеме подключения:
   - схема единой защиты сети;

- схема с защищаемым закрытым и не защищаемым открытым сегментами сети;
- схема с раздельной защитой закрытого и открытого сегментов сети.

Фильтрация трафика

Фильтрация информационных потоков состоит в их выборочном пропускании через экран. Фильтрация осуществляется на основе набора предварительно загруженных в экран правил, соответствующих принятой политике безопасности. МЭ удобно представлять как последовательность фильтров, обрабатывающих информационный поток.

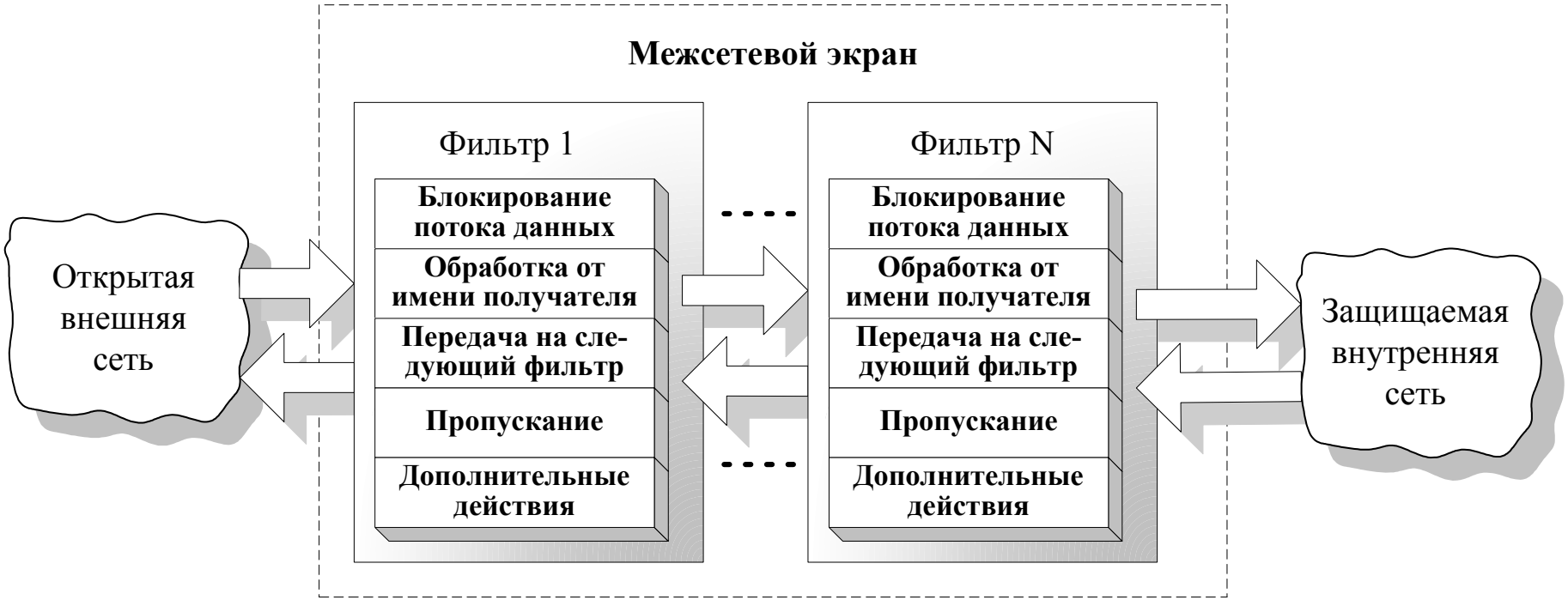


Рис.2. Структура межсетевого экрана

Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации путём выполнения следующих действий:

1. Анализ информации по заданным в правилах критериям (например, по адресам получателя и отправителя).
2. Принятие на основе правил одного из следующих решений:

- не пропускать данные;

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

Правила фильтрации могут задавать дополнительные действия, которые относятся к функциям посредничества (например, преобразование данных, регистрацию событий и т.д.).

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

1. служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и т.д. ;
2. непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие вирусов;
3. внешние характеристики потока информации, например временные и частотные характеристики, объём данных и т.д.

Используемые критерии анализа зависят от уровней модели OSI, на которых осуществляется фильтрация. В общем случае, чем выше уровень модели OSI, на котором МЭ фильтрует пакеты, тем выше обеспечиваемый им уровень защиты.

Выполнение функций посредничества

Функции посредничества МЭ выполняет с помощью специальных программ, называемых экранирующими агентами или программами-посредниками. Обмен информацией между компьютерами

внутренней и внешней сети осуществляется через программного посредника, который может выполнять фильтрацию потока сообщений, и также другие защитные функции.

В общем случае программы посредники могут выполнять следующие функции:

1) проверку подлинности передаваемых данных;
2) фильтрацию и преобразование потока сообщений, например динамический поиск вирусов и прозрачное шифрование информации;
3) разграничение доступа к ресурсам внутренней сети;
4) разграничение доступа к ресурсам внешней сети;
5) кэширование данных, запрашиваемых из внешней сети (proxy–сервер);
6) идентификацию и аутентификацию пользователей;
7) трансляцию внутренних сетевых адресов для исходящих пакетов сообщений;
8) регистрацию событий, реагирование на задаваемые события, генерацию отсчётов и т. д.

Особенности функционирования межсетевых экранов на различных уровнях модели OSI

Комплексный МЭ удобно представлять в виде совокупности неделимых экранов, каждый из которых ориентирован на отдельный уровень модели OSI. При этом функции защиты, выполняемые на разных уровнях эталонной модели, существенно отличаются друг от друга. Чаще всего комплексный МЭ функционирует на сетевом, сеансовом и прикладном уровнях эталонной модели.

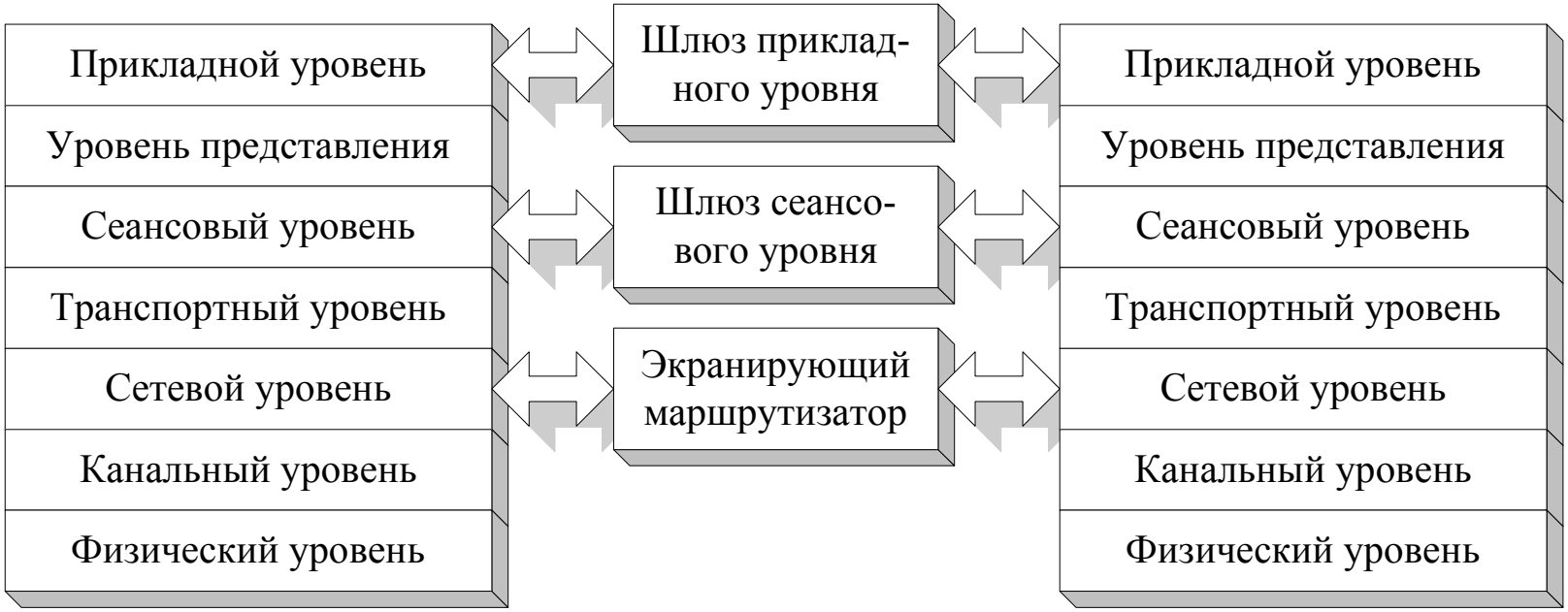


Рис.3.

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 OSI, но может охватывать и транспортный уровень.

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

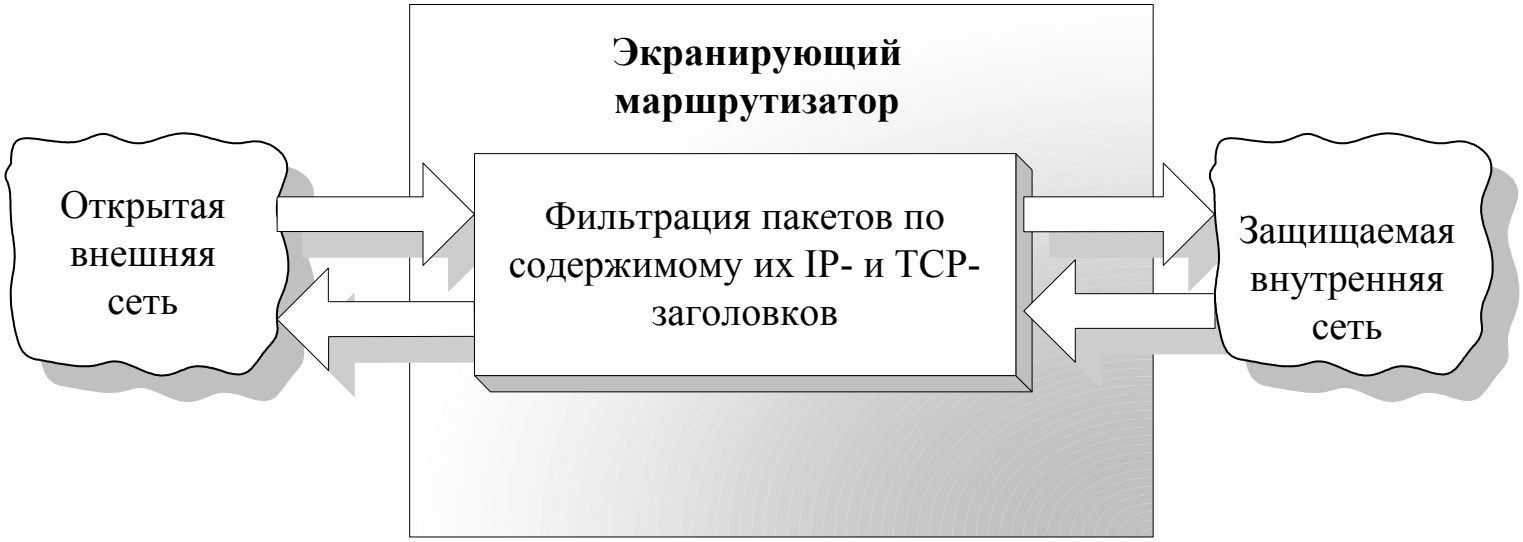


Рис.4. Схема функционирования пакетного фильтра

В качестве анализируемых полей IP– и TCP–заголовков каждого пакета могут использоваться:

1) адрес получателя, адрес отправителя;
2) тип пакета;
3) номер порта получателя и отправителя.

В качестве пакетного фильтра могут быть использованы как обычный маршрутизатор, так и работающая на сервере программа. Современные маршрутизаторы (например, компаний Cisco и Bay Networks) позволяют связывать с каждым портом несколько десятков правил и фильтровать пакеты как на входе, так и на выходе.

Достоинства:

1) простота реализации;
2) высокая производительность;
3) прозрачность для программных приложений;
4) малая цена (обусловлена тем, что любой маршрутизатор в той или иной степени предоставляет возможность фильтрации пакетов).

Недостатки:

1) не обеспечивают высокой степени безопасности (т.к. проверяют только заголовки пакетов и не поддерживают многие необходимые функции защиты – аутентификацию конечных узлов, шифрование, проверку целостности и подлинности);

2) уязвимы для таких сетевых атак, как подмена исходных адресов и несанкционированное изменение содержимого пакетов сообщений.

Шлюз сеансового уровня

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

Контроль виртуальных соединений заключается в слежении за установлением виртуального соединения между рабочей станцией внутренней сети и компьютером внешней сети, а также контроле передачи информации по установленным виртуальным каналам. Такой контроль основывается на информации, содержащейся в заголовках пакетов протокола TCP.

После того, как шлюз определил, что рабочая станция внутренней сети и компьютер внешней сети являются авторизованными участниками сеанса TCP, он устанавливает соединение. При этом шлюз помещает в специальную таблицу соединений соответствующую информацию (адрес отправителя и получателя, состояние соединения и т.д.).

После завершения сеанса, шлюз удаляет соответствующий элемент из таблицы и разрывает цепь, использовавшуюся в данном сеансе (предотвращает фабрикование пакетов после завершения сеанса).

В процессе контроля передачи информации фильтрация пакетов *не осуществляется*. Однако шлюз сеансового уровня способен отслеживать объём передаваемой информации и разрывать соединения после превышения определённого объёма (защита от несанкционированного экспорта информации).

Для контроля виртуальных соединений используются специальные программы, которые называют канальными посредниками (pipe proxies). Канальные посредники ориентированы на конкретные службы TCP/IP (HTTP, FTP, SMTP и т.д.).

Шлюз сеансового уровня также обеспечивает трансляцию внутренних адресов сетевого уровня (IP–адресов) при взаимодействии с внешней сетью. В этом случае, IP–адреса компьютеров внутренней сети автоматически преобразуются в один IP–адрес. В результате, все пакеты, исходящие из внутренней сети, оказываются отправленными МЭ, что исключает прямой контакт между внутренней и внешней сетью и тем самым позволяет скрыть от внешних пользователей структуру внутренней сети.

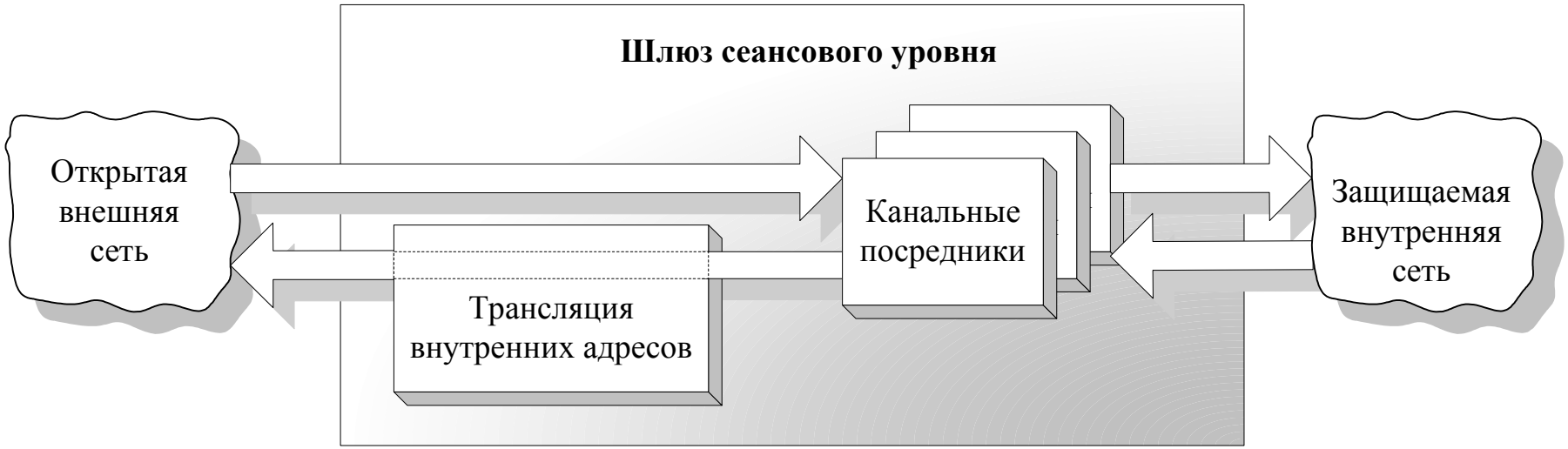


Рис. 5. Схема функционирования шлюза сеансового уровня

Достоинства:

1) представляет собой достаточно простую и относительно надёжную программу с точки зрения реализации;
2) дополняет экранирующий маршрутизатор функциями контроля виртуальных соединений и трансляции внутренних адресов.

Недостатки: те же, что и у экранирующего маршрутизатора.

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

Шлюз прикладного уровня

Шлюз прикладного уровня, называемый также прикладным шлюзом или экранирующим шлюзом, функционирует на прикладном уровне модели OSI, охватывает также уровень представления и обеспечивает наиболее надёжную защиту межсетевых взаимодействий (идентификация и аутентификация, разграничение доступа, поиск вирусов).

Поскольку функции прикладного шлюза относится 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 и т.д.). Программный посредник (application proxy) каждой службы TCP/IP ориентирован на обработку сообщений относящихся только к этой (своей) службы.

Прикладной шлюз перехватывает с помощью соответствующих экранирующих агентов входящие и исходящие пакеты, копирует и перенаправляет информацию, исключая тем самым прямые соединения между внутренней и внешней сетью. Если для какого–либо из приложений отсутствует свой посредник, то прикладной шлюз не сможет обрабатывать трафик такого приложения, и он будет заблокирован.

Фильтрация пакетов сообщений реализуется на прикладном уровне модели OSI. Соответственно, в отличие от канальных посредников, обеспечивается проверка содержимого обрабатываемых пакетов. (Появляется возможность фильтровать отдельные виды команд или информации).

При настройке прикладного шлюза и описании правил фильтрации сообщений используются такие

параметры, как: название сервиса; допустимый временной интервал его использования; ограничения на содержимое сообщений; компьютеры, с которых можно пользоваться сервисом; схемы аутентификации и т.д.

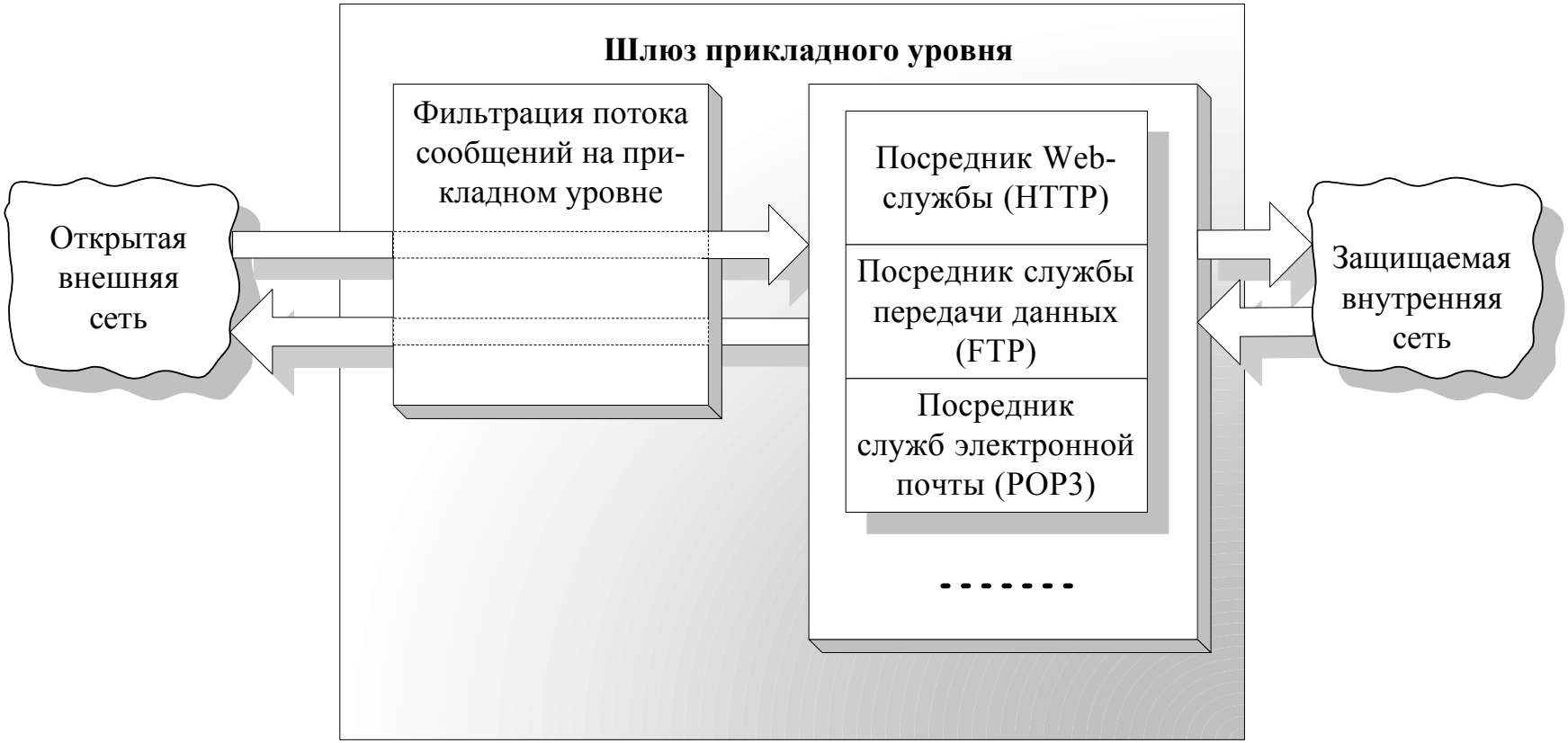


Рис.6. Схема функционирования шлюза прикладного уровня

Достоинства:

1) высокий уровень защиты локальной сети;
2) нарушение работоспособности прикладного шлюза не снижает безопасность защищаемой сети (т.к. блокируется сквозное прохождение пакетов);
3) возможность осуществления большого количества дополнительных проверок.

Недостатки:

1) относительно высокая стоимость;
2) довольно большая сложность МЭ;
3) высокие требования к производительности компьютерной платформы;
4) отсутствие прозрачности для пользователей и снижение пропускной способности при реализации межсетевых взаимодействий.

Критерии оценки качества межсетевых экранов

Общие требования

Межсетевые экраны должны удовлетворять следующим группам требований:

1. По целевым качествам — обеспечивать безопасность защищаемой внутренней сети и полный контроль над внешними подключениями и сеансами связи. Межсетевой экран должен иметь средства авторизации доступа пользователей через внешние подключения. Типичной является ситуация, когда часть персонала организации должна выезжать, например, в командировки, и в процессе работы им требуется доступ к некоторым ресурсам внутренней компьютерной сети организации. Брандмауэр должен надежно распознавать таких пользователей и предоставлять им необходимые виды доступа.

2. По управляемости и гибкости — обладать мощными и гибкими средствами управления для полного воплощения в жизнь политики безопасности организации. Брандмауэр должен обеспечивать простую реконфигурацию системы при изменении структуры сети. Если у организации имеется несколько внешних подключений, в том числе и в удаленных филиалах, система управления экранами должна иметь возможность централизованно обеспечивать для них проведение единой политики межсетевых взаимодействий.

3. По производительности и прозрачности — работать достаточно эффективно и успевать обрабатывать весь входящий и исходящий трафик при максимальной нагрузке. Это необходимо для того, чтобы брандмауэр нельзя было перегрузить большим количеством вызовов, которые привели бы к

нарушению его работы. Межсетевой экран должен работать незаметно для пользователей локальной сети и не затруднять выполнение ими легальных действий. В противном случае пользователи будут пытаться любыми способами обойти установленные уровни защиты.

4. По самозащищенности — обладать свойством самозащиты от любых несанкционированных воздействий. Поскольку межсетевой экран является и ключом и дверью к конфиденциальной информации в организации, он должен блокировать любые попытки несанкционированного изменения его параметров настройки, а также включать развитые средства самоконтроля своего состояния и сигнализации. Средства сигнализации должны обеспечивать своевременное уведомление службы безопасности при обнаружении любых несанкционированных действий, а также нарушении работоспособности межсетевого экрана.

В настоящее время общеупотребительным подходом к построению критериев оценки средств информационно-компьютерной безопасности является использование совокупности определенным образом упорядоченных качественных требований к подсистемам защиты, их эффективности и эффективности реализации. Подобный подход выдержан и в руководящем документе Гостехкомиссии России [2], где устанавливается классификация межсетевых экранов по уровню защищенности от несанкционированного доступа к информации. Данная классификация построена на базе перечня показателей защищенности и совокупности описывающих их требований.

2. Основные классы защищенности межсетевых экранов в соответствии с руководящими документами Гостехкомиссии России

Показатели защищенности применяются к брандмауэрам для определения уровня защищенности, который они обеспечивают при межсетевом взаимодействии. Конкретные перечни показателей определяют классы межсетевых экранов по обеспечиваемой защищенности компьютерных сетей. Деление брандмауэров на соответствующие классы по уровням контроля межсетевых информационных потоков необходимо в целях разработки и принятия обоснованных и экономически оправданных мер по достижению требуемой степени защиты информации при межсетевых взаимодействиях.

Устанавливается пять классов межсетевых экранов по показателям защищенности. Самый низкий класс защищенности — пятый, применяемый для безопасного взаимодействия автоматизированных систем класса 1Д с внешней средой, четвертый — для 1Г, третий — 1В, второй — 1Б, самый высокий — первый, применяемый для безопасного взаимодействия автоматизированных систем класса 1А с внешней средой. При включении брандмауэра в автоматизированную систему (АС) определенного класса защищенности, класс защищенности совокупной системы, полученной из исходной путем добавления в нее межсетевого экрана, не должен понижаться. Для АС класса 3Б, 2Б должны применяться брандмауэры не ниже 5-го класса. Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться брандмауэры следующих классов:

- при обработке информации с грифом "секретно" — не ниже 3-го класса;

- при обработке информации с грифом "совершенно секретно" — не ниже 2-го класса;
- при обработке информации с грифом "особой важности" — не ниже 1-го класса.

Вспомним, что в соответствии с руководящим документом Гостехкомиссии России [3], устанавливается девять классов защищенности АС от несанкционированного доступа к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС. Класс, соответствующий высшей степени защищенности для данной группы, обозначается индексом NA, где N — номер группы от 1 до 3. Следующий класс обозначается NБ и т. д.

Третья группа включает АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Данная группа содержит два класса 3Б и 3А. Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и/или хранимой на носителях различного уровня конфиденциальности. Эта группа содержит два класса 2Б и 2А. Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и/или хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Данная группа содержит пять классов 1Д, 1Г, 1В, 1Б и 1А. Требования к межсетевым

экранам по классам защищенности приведены в табл. 2.

Таблица 1. Перечень показателей межсетевых экранов по классам защищенности

Показатели защищенности	**5**	**4**	**3**	**2**	**1**
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	–	–	+	=	+
Регистрация	–	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	–	–	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	=

Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Обозначения:
"-" — нет требований к данному классу;
"+" — новые или дополнительные требования;
"=" — требования совпадают с требованиями к МЭ предыдущего класса.

Обзор современных межсетевых экранов

Технологии виртуальных частных сетей VPN.

- Классификация VPN.
- Протокол защиты сетевого уровня IPSe.
- Протоколы формирования защищенных каналов на сеансовом уровне SSL/TLS.
- Протоколы формирования защищенных каналов на канальном уровне L2F и L2TP. Примеры настройки и работы защищённых туннелей.

1. Назначение VPN

При подключении локальной сети организации к открытой сети возникают угрозы безопасности двух основных типов:

- несанкционированный доступ к внутренним ресурсам локальной сети, получаемый злоумышленником в результате несанкционированного входа в эту сеть;
- несанкционированный доступ к данным в процессе их передачи по открытой сети.
- Обеспечение безопасности информационного взаимодействия локальных сетей и отдельных компьютеров через открытые сети возможно путем эффективного решения следующих задач:
- защита подключенных к открытым каналам связи локальных сетей и отдельных компьютеров

от несанкционированных действий со стороны внешней среды;

- защита информации в процессе ее передачи по открытым каналам связи.

Для защиты локальных сетей и отдельных компьютеров от несанкционированных действий со стороны внешней среды обычно используют межсетевые экраны (firewalls), поддерживающие безопасность информационного взаимодействия путем фильтрации двустороннего потока сообщений, а также выполнения функций посредничества при обмене информацией.

Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN.

2. Основные определения

Виртуальной защищенной сетью VPN (Virtual Private Network) называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную сеть, обеспечивающую безопасность циркулирующих данных.

Виртуальная защищенная сеть VPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются туннелями VPN.

Туннель VPN представляет собой соединение, проведенное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети.

Защита информации в процессе ее передачи по туннелю VPN основана на выполнении следующих функций:

- аутентификации взаимодействующих сторон;
- криптографического закрытия (шифрования) передаваемых данных;
- проверки подлинности и целостности доставляемой информации.

Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем. Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, причем эта защищенная выделенная линия развертывается в рамках общедоступной сети, например Internet.

Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN.

3. Принцип туннелирования

Для безопасной передачи данных через открытые сети широко используют инкапсуляцию и туннелирование. С помощью методики туннелирования пакеты данных передаются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель-получатель данных» устанавливается своеобразный туннель – логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого.

Суть туннелирования состоит в том, чтобы инкапсулировать, то есть «упаковать» передаваемую порцию данных, вместе со служебными полями, в новый «конверт». При этом пакет протокола более низкого уровня помещается в поле данных пакета протокола более высокого или такого же уровня. Следует отметить, что туннелирование само по себе не защищает данные от несанкционированного доступа или искажения, но благодаря туннелированию появляется возможность полной криптографической защиты инкапсулируемых исходных пакетов.

Чтобы обеспечить конфиденциальность передаваемых данных, отправитель шифрует исходные пакеты, упаковывает их во внешний пакет с новым IP-заголовком и отправляет по транзитной сети

Особенностью туннелирования является то, что эта технология позволяет зашифровать исходный пакет целиком вместе с заголовком, а не только его поле данных. Это важно, поскольку некоторые поля заголовка содержат информацию, которая может быть использована злоумышленником. В частности, из заголовка исходного пакета можно извлечь сведения о внутренней структуре сети – данные о количестве подсетей и узлов и их IP-адресах.

4. Основные компоненты виртуальной частной сети

Защищенный туннель создается компонентами виртуальной сети, функционирующими на узлах, между которыми формируется туннель. Эти компоненты принято называть инициатором туннеля и терминатором туннеля.

Инициатор туннеля инкапсулирует исходный пакет в новый пакет, содержащий новый заголовок с информацией об отправителе и получателе. Инкапсулируемые пакеты могут принадлежать к протоколу любого типа, включая пакеты немаршрутизируемых протоколов, например NetBEUI. Все передаваемые по туннелю пакеты являются пакетами IP. Маршрут между инициатором и терминатором туннеля определяет обычная маршрутизируемая сеть IP, которая может быть отличной от Internet.

Инициировать и разрывать туннель могут различные сетевые устройства и программное обеспечение. Например, туннель может быть инициирован ноутбуком мобильного пользователя, оборудованным модемом и соответствующим программным обеспечением для установления соединений удаленного доступа. В качестве инициатора может выступить также маршрутизатор локальной сети, наделенный соответствующими функциональными возможностями. Туннель обычно завершается коммутатором сети или шлюзом провайдера услуг.

Терминатор туннеля выполняет процесс, обратный инкапсуляции. Терминатор удаляет новые заголовки и направляет каждый исходный пакет адресату в локальной сети.

5. Критерии безопасности данных в сетях VPN

Применительно к задачам VPN критерии безопасности данных могут быть определены следующим образом:

- *конфиденциальность* – гарантия того, что в процессе передачи данных по защищенным

каналам VPN эти данные могут быть известны только легальным отправителю и получателю;

- *целостность* – гарантия сохранности передаваемых данных во время прохождения по защищенному каналу VPN. Любые попытки изменения, модификации, разрушения или создания новых данных будут обнаружены и станут известны легальным пользователям;
- *доступность* – гарантия того, что средства, выполняющие функции VPN, постоянно доступны легальным пользователям. Доступность средств VPN является комплексным показателем, который зависит от ряда факторов: надежности реализации, качества обслуживания и степени защищенности самого средства от внешних атак.

Конфиденциальность обеспечивается с помощью различных методов и алгоритмов симметричного и асимметричного шифрования. Целостность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на асимметричных методах шифрования и односторонних функциях.

Аутентификация осуществляется на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт, протоколов строгой аутентификации и обеспечивает установление VPN-соединения только между легальными пользователями, предотвращая доступ к средствам VPN нежелательных лиц. Авторизация подразумевает предоставление абонентам, доказавшим свою легальность (аутентичность), различных видов обслуживания, в частности разных способов шифрования их трафика. Авторизация и управление доступом часто реализуются одними и теми же средствами.

Для обеспечения безопасности передаваемых данных в виртуальных защищенных сетях должны быть решены следующие основные задачи сетевой безопасности:

- взаимная аутентификация абонентов при установлении соединения;
- обеспечение конфиденциальности, целостности и аутентичности передаваемой информации;
- авторизация и управление доступом;
- безопасность периметра сети и обнаружение вторжений;
- управление безопасностью сети.

Технологии анализа защищенности.

- Средства анализа защищенности сетевых протоколов и сервисов.
- Технологии обнаружения сетевых атак: методы анализа сетевой информации, классификация систем обнаружения атак, компоненты и архитектура системы обнаружения атак.
- Особенности систем обнаружения атак на сетевом и операционном уровнях.
- Методы реагирования на атаки.
- Обзор современных средств обнаружения атак.