Государственное бюджетное профессиональное образовательное учреждение города Москвы

«Колледж современных технологий им. М. Панова»

**КУРСОВАЯ РАБОТА**

На тему: «**Анализ проблем информационной безопасности в компьютерной сети, организации подключенной к сети Интернтет**»

Выполнил:

Студент   
2 курса, группы СОБ-215, Грачев Григорий Юрьевич

Научный руководитель:

Грибаков Сергей Леонидович

Москва, 2020

**Содержание**

Введение

1. Анализ проблем информационной безопасности организации, присоединенной к сети Интернет. Актуальные на сегодня подходы к их решению

1.1 Экспертный анализ информационной безопасности современных компьютерных сетей организации

1.2 Вопросы информационных безопасности интернет – сервисов

1.3 Методы защиты компьютерной сети организации от НСД из сети Интернет. Применение межсетевых экранов

2. Теоретические вопросы построения межсетевых экранов

2.1 Архитектуры межсетевых экранов

2.2 Классификация межсетевых экранов

2.3 Уровень защищенности межсетевых экранов

3 Intrusion Detection Systems (IDS)

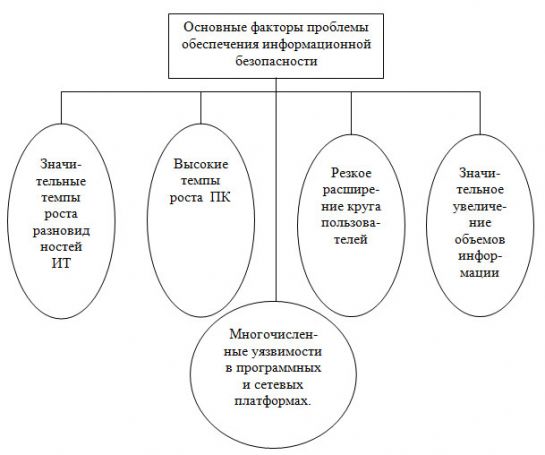
3.1 IPv6 как сильное влияние на конструкцию межсетевого экрана

Заключения

Список сокращений и обозначений

Список использованных источников литературы

**Введение**

В настоящее время компьютеры, сети, интернет стали обязательной составляющей нашей обыденной жизни. Наш быстроразвивающийся, наполненный технологиями мир с каждым днем все больше становится зависимым от компьютерных технологий, а также сетей. Но данная зависимость возникла не внезапно. С каждым годом субсидирование компьютерных технологий заметно возрастало, и это совсем не удивительно, что эти технологические процессы проникли практически во все без исключения области деятельности человека.   
  
На заре формирования компьютерных технологий большая часть людей никак не имели возможность представить, насколько широко эти технологии станут применяться в будущем. Поэтому, многие не решались уделять большое количество времени и усилий для изучения того, что в конце концов могло быть обыкновенной забавой. Согласно сравнению, с условиями нынешнего рынка работы число людишек, трудившихся во в таком случае период во сфере компьютерных технологий, было ничтожно мало. Люди, работавшие в данном тесном сообществе, были хорошо знакомы и верили друг другу. Помимо того, в это объединение допускались только избранные, которые заслуживали доверия. Таким образом, в эти времена проблемы безопасности в области компьютерных технологий практически отсутствовали. И довольно длительное период времени специалисты в области компьютерных технологий не уделяли внимания безопасности компьютерных сеток.   
  
Во наше время период новые информационные технологические процессы стремительно внедряются во всех сферах государственной экономики. Возникновение локальных и глобальных сетей передачи данных предоставило юзерам ПК новейшие возможности оперативного обмена данными. Если до недавнего времени аналогичные сети формировались только лишь в специфических и узконаправленных целях, то формирование интернета и подобных систем привело к применению глобальных сетей передачи данных в повседневной жизни почти каждого человека. 

**1. Анал лизь проблем информационной безопасности оргазмизации, присоединенной к сети Интернет. Актуальные на сегодня подходы к их решению**

**1.1 Экспертный анализ информационной безопасности современных компьютерных сетей организации**

Развитие информационных технологий, а также их повсеместное проникновение в самые различные сферы деловой деятельности привело к тому, что компьютерная информация может иметь вполне определенную стоимость. По этой причине одна из основных проблем формирования информационных технологий на предприятии и организации — надежное предоставление информационной безопасности. Ее решение — исследование форм, методов, а также технологий выявления и предотвращения опасности в информационной сфере, а кроме того руководство информационной безопасностью на предприятии, подбор средств защиты. Деятельность согласно защите охраняемой владельцем информации, в основную очередь, сопряжена с предупреждением утечки секретной информации. Согласно указу Президента РФ, выделяют виды конфиденциальной информации: служебная тайна, персональные данные, тайна следствия и судопроизводства, адвокатская, нотариальная, коммерческая тайна, тайна сущности изобретения до момента опубликования, профессиональная тайна, тайна связи, банковская, врачебная, налоговая тайна.

Значимость и важность трудности предоставления информационной

Безопасности обусловлены последующими факторами:

• Необходимые на сегодняшний день уровни и темпы формирования информационной безопасности во многом отстают от уровней темпов развития информационных технологий.

• Высокие темпы увеличения парка личных пк, применяемых в различных областях человеческой деятельности.

• Существенное повышение размеров данных, накапливаемой, хранимой и обрабатываемой с помощью компьютеров и иных ресурсы автоматизации;

• Множественные уязвимости во программных также сетевых платформах;

Активное развитие информативных технологий открыло ранее не известные потенциал со целью коммерции, но повергло кроме этого к возникновению ранее не известных угроз. Инновационные программные продукты питания из-за конкурентной борьбы оказываются во реализацию с погрешностями также недоработками. До тех пор, пока не станут разрешены данные проблемы, недостаточного уровня информативной безопасности это будет существенным тормозом в создании информативных технологий.

• Активное формирование всемирной Сеть Интернет, почти никак не мешающей нарушениям защищенности систем обрабатывания данных в абсолютно во всем мире.

• Инновационные способы накапливания и передачи данных поспособствовали возникновению угроз, связанных с перспективой утраты, искажение, а также раскрытия информации, которые принадлежат конечным юзерам.

Реализация той или иной угрозы безопасности может преследовать следующие цели:

• Несоблюдение конфиденциальности данных. Сведения обрабатываемая в компьютерной сети организации (КСО), способен обладать крупной ценностью для ее собственника. Использование этой информации другими лицами, наносит существенный вред интересам собственника;

• Несоблюдение целостности данных. Утрата целостности данных - риск её раскрытия. Значимые сведения могут быть утрачены, либо обесценена линией ее неразрешенного удаления, либо изменения. Вред с подобных операций может являться может быть много больше, чем при нарушении конфиденциальности;

• несоблюдение работоспособности КСО. Вывод из строя либо некорректное изменение систем деятельность компонентов КСО, их модификация или замена могут послужить причиной к получению неверных результатов, отказу КСО от потока информации или отказам при обслуживании. Отклонение от потока информации обозначает непризнание одной с взаимодействующих сторон факта передачи или же приема сообщений. Имея в виду, то что подобные сообщения могут заключать в себе важные донесения, заказы, финансовые согласования и т.п., ущерб в этом случае может быть колоссальным.

Следовательно, обеспечивание информативной защищенности компьютерных систем также сетей считается один из основных течений формирования информативных технологий.

Коллективная информационная система — информационная концепция, соучастниками которой может являться небольшой круг лиц, конкретный ее собственником (с закона о Электронно-числовой подписи).

Компьютерные сети организации (КСО) принадлежат к распределенным компьютерным концепциям, исполняющим автоматизированную обрабатывание данных. Проблема предоставления информативной защищенности считается основной с целью подобных компьютерных концепций. Обеспечение защищенности КСО подразумевает систему противодействия каждому несанкционированному проникновению в действие функционирования КСО.

Систематизация предприятий с точки зрения ИБ

С Целью установления принадлежности предприятия к тому или другому классу, ведется исследование соотношения согласно последующим характеристикам для каждого вида

1) Применение ИТ в предпринимательском процессе – уровень с которой предприятия используют ИТ в критичных для производство процессах

2) Технологический профиль– разновидности технологий, применяемых предприятием, ранжируя их с автономных компьютеров до универсальных ЭВМ (mainframe)

3) Установление доверия– процесс, применяемый предприятием с целью налаживания отношений со своим деловым партнером, т.е. “Знаю Ваш Клиент”

4) Информационная важность актива за пределами предприятия, или "Значение для Хакера”– ценность для хакера/внешней стороны, по взаимоотношению к предприятию, информационных активов если

5) Покрытие ИБ– персонал и управление в месте, необходимые, для того чтобы обезопасить информационные активы предприятия

6) Удар при прорыве безопасности – воздействование на предприятие, в случае если безопасности была нарушена Gartner Group акцентирует внимание на 4 уровня зрелости фирмы с точки зрения обеспечения информационной безопасности (ИБ)

|  |  |
| --- | --- |
| 0 уровень | ИБ в компании никто не занимается, руководство компании не осознает важности проблем ИБ;  Финансирование отсутствует;  ИБ реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам). |
| 1 уровень | ИБ рассматривается руководством как чисто "техническая" проблема, отсутствует единая программа (концепция, политика) развития системы обеспечения информационной безопасности (СОИБ) компании;  Финансирование ведется в рамках общего ИТ-бюджета;  ИБ реализуется средствами нулевого уровня + средства резервного копирования, антивирусные средства, межсетевые  экраны, средства организации VPN (традиционные средства защиты). |
| 2 уровень | ИБ рассматривается руководством как комплекс организационных и технических мероприятий, существует понимание важности ИБ для производственных процессов, есть утвержденная руководством программа развития СОИБ компании;  Финансирование ведется в рамках отдельного бюджета;  ИБ реализуется средствами первого уровня + средства усиленной |
|  | аутентификации, средства анализа почтовых сообщений и web- контента, IDS (системы обнаружения вторжений), средства анализа защищенности, SSO (средства однократной аутентификации), PKI (инфраструктура открытых ключей) и организационные меры (внутренний и внешний аудит, анализ риска, политика информационной безопасности, положения,  процедуры, регламенты и руководства). |
| 3 уровень | ИБ является частью корпоративной культуры, назначен CISA (старший офицер по вопросам обеспечения ИБ);  Финансирование ведется в рамках отдельного бюджета;  ИБ реализуется средствами второго уровня + системы управления ИБ, CSIRT (группа реагирования на инциденты нарушения ИБ), SLA (соглашение об уровне сервиса). |

По информации Gartner Group процентное соотношение компаний применительно к описанным 4 уровням выглядит следующим образом:

|  |  |  |
| --- | --- | --- |
| 2001 год | 2005 год | 2008 год |
| 0 уровень - 30% | 0 уровень - 20% | 0 уровень – 5 % |
| 1 уровень - 55% | 1 уровень - 35% | 1 уровень – 40 % |
| 2 уровень - 10 % | 2 уровень - 30 % | 2 уровень – 35 % |
| 3 уровень - 5 % | 3 уровень - 15 % | 3 уровень – 20 % |

Таким методом, основательный подход к задачам обеспечения ИБ возникает исключительно на вторых и третье уровне. А на первом также в нулевом степени зрелости в согласовании с этой систематизации обладает роль таким образом именуемый «фрагментарный» подход к обеспечению ИБ. «Фрагментарный» подход ориентирован в сопротивление определенным угрозам в установленных обстоятельствах. В качестве примеров осуществлении подобного подхода можно определить единичные средства управления допуском, независимые средства кодирования, антивирусные программы и т.п.

Преимущество предоставленного подхода состоит в существенной избирательности к конкретной опасности. Минусом данного подхода считается недостаток общей защищенности данных. Фрагментарные меры защиты данных гарантируют охрану определенных объектов КС только лишь с конкретной угрозы. Наиболее основательные компании, подходящие второму, а также третьему уровню зрелости систематизации Gartner, используют «комплексный» отношение к обеспечению ИБ. Данный подход предлагает серьезные фирмы, которые профессионально специализируются на защите информации.

Систематический подход базируется на решении комплекса индивидуальных задач согласно единому плану. Данный подход в наше время признается главным для формирования защищенной среды обрабатывания данных в корпоративных системах, сводящей в одно единое разные планы противодействия угрозам. Сюда относятся правовые, морально этические, организационные, программные и технические методы предоставления информативной безопасности. Систематический подход предоставил совместить целый ряд независимых систем путем их интеграции в так называемые встроенные концепции защищенности.

Способы решения вопросов обеспечения защищенности непосредственно связаны с уровнем формирования науки и техники, в особенности с уровнем научно-технического обеспечения. Но отличительной направленностью формирования нынешних технологий считается процесс полной интеграции. Данной направленностью охвачены микроэлектроника, а также оборудование связанной с технической связью.

Дальнейшим формированием единого подхода или его наибольшей конфигурацией считается совокупный подход, основанный на интеграции разных подсистем предоставления защищенности, подсистем связи в общую накопленную концепцию с техническими средствами, каналами связи, программным обеспечением и базами данных. Совокупный подход ориентирован на результат накопленной безопасности. Главное значение определения накопленной защищенности заключается в потребности обеспечить подобное положение условий функционирования компании, при котором она защищена от всех допустимых видов опасностей в процессе всего постоянного производственного процесса. Понятие накопленной безопасности подразумевает неотъемлемую беспрерывность процесса предоставления безопасности, как во времени, так и в пространстве, с неотъемлемым учетом абсолютно всех вероятных разновидностей угроз.

В какой-либо бы форме ни использовался систематический, либо совокупный подход, он постоянно ориентирован на разрешение ряда индивидуальных вопросов в их близкой связи с применением единых технических средств, каналов взаимосвязи, программного обеспечения. К Примеру, применительно к информативной защищенности наиболее очевидными из них считаются проблемы допуска к информации, технологического, а также криптографического закрытия данных.

**1.2 Вопросы информационных безопасности интернет – сервисов**

Всемирная паутина World Wide Web

WWW стала одной из ключевых факторов взрывного расширения Интернет в последние годы. Фактором ее популярности стала вероятность интерактивного доступа к сведениям различных видов, в этом числе гипертексту, графике, аудио, видеоматериал и т.д. World wide web представляет из себя большое количество HTTP-серверов в Интернет.

Трудности защищенности HTTP-клиентов объединены с их расширяемостью. Так как интернет-серверы предоставляют сведения в почти всех форматах (обычный текст, HTML, графические файлы gif и jpeg, аудио файлы и др.), с целью воспроизведения разных форматов браузеры активизируют наружные дополнения.

Обычного решения вопросов безопасности, связанных с интенсивными элементами и иным исполняемым кодом, загружаемым, с www не имеется. Способы борьбы с проблемами содержат в себе подготовку юзеров и разъяснение им вопросов безопасности, сопряженных с загружаемым из сети исполняемым кодом, отключение в клиентском программном обеспечении способности выполнения загружаемых действующих элемент, своевременное обновление абонентного ПО с целью корректировки зафиксированных в нем ошибок и т.п.

Электронная почта

Электрическая почта считается популярной и интенсивно используемой службой. Она представляет относительно небольшой риск, однако, этот риск не стоит не до оценивать.

Главные проблемы, сопряженные со электронной почтой:   
• фальсификация электрической почты. Протокол SMTP, применяемый с целью передачи электронной почты в Интернет не предоставляет средств аутентификации отправителя. Местоположение отправителя письма может быть подделанным подделан.   
• передача исполняемого кода в почтовых сообщениях. Электронная почта дает возможность передавать сведения различных видов, в том числе и программы. Совместно с подделкой адреса отправителя — это может применяться с целью различных атак.   
• перехват почтовых сообщений. Электронная почта переходит посредством Интернет в не зашифрованном облике, также может быть перехвачена и обнародована.   
• Спам. Спамом называется многочисленное распространение уведомлений маркетингового характера. FTP - протокол передачи файлов

Протокол FTP применяется с целью передачи файлов. Большая Часть web-броузеров прозрачно поддерживают FTP. Можно также использовать специализированные FTP-клиенты.

Главный проблемой, как и в случае www считаются программы, выкачиваемые и устанавливаемые юзерами, которые имеют все шансы нести вредоносный характер.

DNS - доменная система имен

DNS - доменная система имен - изменение имена в адреса и в обратном порядке. Все Без Исключения программы, которые применяют с целью обращения к отдаленным хостам имена, являются DNS-клиентами. DNS считается основной службой, которую применяют прочие службы с целью собственной деятельности.

DNS функционирует следующим образом: клиент отправляет запрос локальному серверу (к примеру, запрашивает IP-адрес www.microsoft.com). Сервер проверяет, имеется ли у него данные сведения в кэше, и, в случае если отсутствует, DNS-сервер запрашивает прочие DNS-сервера по очереди, для того чтобы получить результат на требование клиента. Если DNS-сервер получает результат, он решение, что ответ получить невозможно, он кэширует полученную информацию и передает ответ клиенту.

Проблемы безопасности DNS:

• Раскрытие информации. DNS может проинформировать потенциальному взломщику больше данных, нежели необходимо, к примеру, имена и адреса внутренних серверов, а также работников станций.

• Погрешности в программном коде DNS-сервера. В 1998 г. во широко используемом DNS-сервере BIND было обнаружено несколько ошибок, одна из которых позволяла получить удаленному взломщику привилегированный (root) доступ к системе. Эти ошибки существовали исправлены в следующих версиях.

**1.3 Методы защиты компьютерной сети организации от НСД из сети Интернет. Применение межсетевых экранов**

Есть несколько подходов к решению проблемы защиты КСО присоединенной к узы Интернету от НСД. 1-Ый подход заключается в усилении охраны абсолютно всех иметься в наличии систем, открытых к доступу из сети. Данный подход называется "безопасность на уровне хоста". Он способен содержать в себе обучение юзеров и администраторов систем работе в наиболее враждебной среде, ужесточение политики парольной защиты либо внедрение не парольных способов аутентификации, ужесточение правил допуска к системам, усиление требований к используемому программному обеспечению, в том числе операционным системам, и систематическая контроль исполнения всех установленных требований.

У этого подхода имеется ряд недостатков:

• для пользователей усложняются работа в системе, и возможно, некие операции к которым они привыкли, вообще запрещены. Это может послужить причиной к уменьшению производительности пользователей, а также к их недовольству.

• на администраторов системы возлегает дополнительная работа по поддержке системы.

• требования защиты имеют все шансы, быть в противоречии требованиям использования системы и одним из них придется отдать предпочтение в ущерб остальным. Равно как правило, требованиям к функциональности системы отдается преимущество во вред требования защиты.

Плюсом данного расклада считается то, что кроме проблемы защиты от "внешнего врага" он также решает вопрос внутренней безопасности системы. Поскольку существенная доля инцидентов (по некоторым сведениям, вплоть до 80%), связанных с защищенностью, исходит от работников или бывших сотрудников компаний, этот подход способен крайне результативно увеличить единую безопасность системы.

2-Ой подход считается более действенным. В нем рабочая сеть компании на физическом уровне не связана с Интернетом. Для взаимодействия с Интернетом применяется одна или ряд специально выделенных машин, не включающих никакой секретной информации. Плюсы данного подхода бесспорны: так как рабочая сеть не соединена с Интернетом, угроза НСД из сети Интернет для нее нет в принципе. Минусы данного подхода проистекают из наличия незащищенных систем, подсоединенных к Интернету, которые имеют все шансы подвергаться атакам типа "отказ в обслуживании", и краже услуг.

3-Ий подход, именуемый "безопасность на уровне сети" заключается в внедрении средств ограничения допуска в точке соединения сетей. Данный подход дает возможность сосредоточить ресурсы защиты и контроля в точках объединения 2-ух и более сетей, к примеру, в точке соединения КСО с Интернетом.

Согласно определению Государственной Технической Комиссии при Президенте Российской Федерации “Межсетевой экран представляет собой локальное или высоко функционально-распределенное средство, реализующее надзор за данными, поступающей в автоматизированную систему и/или сходящей с автоматизированной концепции, также гарантирует охрану автоматизированной концепции с помощью фильтрации данных, т.е. ее анализа согласно совокупности критериев и принятия постановления о ее распространении в "автоматизированную систему”. Межсетевые экраны, при правильном их применении, считаются крайне результативным средством защиты от угроз корпоративным сетям, исходящим из сети Интернет.

**2. Теоретические вопросы построения межсетевых экранов**

**2.1 Архитектуры межсетевых экранов**

Межсетевое экраны смогут быть сконфигурированы в типе одной из многих архитектур, что гарантирует различные уровни безопасности при всевозможных затратах на установку и поддержание работоспособности. Организации обязаны рассмотреть свой профиль риска и подобрать подходящую архитектуру. Ниже описываются характерные архитектуры межсетевого экрана и приводят примеры политик безопасности для них.

Хост, подключенный к 2 сегментам сети:

Это такой хост, который содержит более 1-го интерфейса с сетью, при этом любой интерфейс с сетью включен физически к отдельному сегменту сети. Часто встречаемым примером является хост, подключенный к 2 сегментам.

Межсетевой экран на основе хоста, подключенного к 2 сегментам сети - данный межсетевой экран с 2-мя сетевыми платами, каждая из которых подключена к отдельной сети. К Примеру, одна сетевая плата соединена с внешней или небезопасной сетью, а вторая - с внутренней или безопасной сетью. В данной конфигурации основным принципом предоставления безопасности считается запрещение непосредственный маршрутизации трафика из не доверенной сети в доверенную – межсетевой экран все время должен оставаться при этом промежуточным звеном.

Маршрутизация должна быть отключена в межсетевом экране такого типа, чтобы IP-пакеты из одной сети не имели возможность проделать путь в другую сеть.

Подобная структура, скорее всего, является одной из наиболее недорогих и распространенных при коммутируемом подключении ЛВС организации к сети Интернет. Берется машина, на которую устанавливается FreeBSD, и на ней запрещается маршрутизация, помимо того надлежащим способом настраивается интегрированный в ядро пакетный фильтр (ipfw).

Экранированный хост:

При архитектуре типа экранированный хост применяется хост (называемый хостом-бастионом), с которым может установить связь каждой внешний хост, однако запрещен допуск ко всем другим внутренним, менее безвредным хостам. Для этого фильтрующий маршрутизатор настраивается таким образом, то что все объединения с внутренней сетью из наружных сетей направляются к хосту-бастиону.

Если шлюз с пакетной фильтрацией установлен, то хост-бастион обязан быть сконфигурирован так, чтобы все объединения из наружных сетей шли через него, для того чтобы избежать прямое объединение между компьютерной сетью организации и узы Интернетом.

Экранированная подсеть:

Архитектура экранированной сети по сути схож с архитектурой экранированного хоста, однако добавляет еще 1 линию защиты, с помощью формирования сети, в которой присутствует хост-бастион, изолированной от внутренней сети.

Экранированная подсеть обязана внедряться с помощью присоединения сети-периметра для того, чтобы разделять внутреннюю сеть от внешней. Это дает гарантию, что даже при успехе атаки в хост-бастион, атакующий никак не сумеет проделать путь дальше сети-периметра из-за того, что между внутренней сетью и сетью-периметром располагается еще один экранирующий маршрутизатор.

**2.2 Классификация межсетевых экранов**

Межсетевые экраны являются устройствами или системами, которые управляют потоком сетевого трафика между сетями с разными требованиями к защищенности. В основной массе нынешних приложений межсетевые экраны, а также их окружения обсуждаются в контексте сочетаний в Интернете и, таким образом, применения стека протоколов TCP/IP. Но межсетевые экраны используются также в сетевых окружениях, которые никак не требуют непременного подсоединения к Интернету. К Примеру, многочисленные корпоративные сети предприятия устанавливают межсетевые экраны с целью имитирования соединений из также внутренних сетей, обрабатывающие информацию разного уровня восприимчивости, подобную как бухгалтерская информация либо сведения о заказчиках. Определяя межсетевые экраны с целью контролирования соединений с этими областями, организация может избежать не авторизованный допуск к надлежащим системам и ресурсам изнутри чувствительных областей. Этим наиболее, применение межсетевого экрана гарантирует вспомогательный уровень защищенности, который по-другому никак не может быть достигнут.   
  
В наше время существует ряд видов межсетевых экранов. Одним из методов сравнения их способностей считается перечисление уровней модели OSI, которые данный тип межсетевого экрана способен подвергать анализу- Модель OSI считается абстракцией сетевого взаимодействия между компьютерными системами и сетевыми приборами. Проанализируем только уровни модели OSI принадлежащие к межсетевым экранам. В рис. 2.1 показана стек протоколов модели OSI.

|  |
| --- |
| https://www.bestreferat.ru/images/paper/16/58/7365816.png |

Рис.2.1. Стек протоколов модели OSI

Уровень 1 предполагает собою реальную аппаратуру физического соединения и среду, подобную равно как Ethernet.   
Уровень 2 — степень, на котором сетевой трафик переходит согласно локальной сети (LAN). Он кроме того считается первоначальным уровнем, владеющим возможностью адресации, с поддержкой которой возможно распознать отдельную машину. Адреса назначаются в сетевые интерфейсы и называются MAC (Media Access Control) адресами. Ethernet - адрес, являющийся собственностью Ethernet-карте, считается образцом МАС - адреса уровня 2.   
Уровень 3 считается степенью, отвечающим за доставку сетевого трафика согласно WAN. Во Сети Интернет адреса уровня 3 называют IP-адресами; адреса как правило считаются уникальными, однако присутствие определенных обстоятельствах, к примеру, присутствие трансляции сетевых адресов (NAT) возможны ситуации, если разнообразные физические системы обладают один и тот же IP-адрес уровня 3.   
Уровень 4 определяет конкретное сетевое приложение и коммуникационную сессию в добавок к сетевым адресам; система способена обладать огромное количество сессий уровня 4 с иными ОС. Терминология, сопряженная с семейством протоколов TCP/IP, содержит представление портов, которые имеют все шансы рассматриваться равно как окончательные точки сессий: номер порта ключа устанавливает коммуникационную сессию в исходной системе; номер порта назначения устанавливает коммуникационную сессию системы назначения. Наиболее высокие уровни (5, 6, а также 7) представляют приложения и системы конечного юзера.

Мостиковые межсетевые экраны - это группа межсетевого экрана, действующий на 2-м степени модели OSI, известен также как прозрачный (stealth), скрытый, теневой межсетевой экран.   
  
Ко плюсам аналогичных межсетевых экранов можно отнести:   
• Отсутствует потребности в изменении опций корпоративной сети, не требуется вспомогательного конфигурирования сетевых интерфейсов межсетевого экрана.   
• Высокая производительность. Так как это элементарные устройства, они не требуют крупных расходов ресурсов. Ресурсы требуются либо с целью увеличения способностей машин, или с целью наиболее углубленного анализа информации.   
• Прозрачность. Основным для данного устройства считается его функционирование на 2 уровне модели OSI. Это значит, то что общесетевой интерфейс никак не обладает IP-адреса. Данная отличительная черта наиболее значима, нежели простота в настройке. В Отсутствии IP-адреса данное устройство не открыто в сети и считается невидимым для окружающего мира. В Случае Если такого рода межсетевой экран недоступен, в таком случае как его атаковать? Атакующие даже не будут знать, то что имеется межсетевой экран, контролирующий любой их пакет.

Фильтрующие маршрутизаторы:  
Межсетевой экран с фильтрацией пакетов (Packet - filtering firewall) - межсетевой экран, который считается маршрутизатором либо пк, на котором функционирует программное обеспечение, сконфигурированное подобным способом, для того чтобы отфильтровывать конкретные виды входящих и исходящих пакетов. Фильтрация пакетов исполняется на основе данных, содержащейся во TCP- IP-заголовках пакетов.  
  
• Работают на 3 уровне   
• Кроме Того известны, как межсетевой экран на основе порта   
• Любой комплект сравнивается с перечнями правил (адрес источника/получателя, порт источника/получателя)   
• Доступный По Цене, быстрый (эффективный), однако менее защищенный   
• Технология 20-летней давности   
• Пример: список контроля доступа (ACL, access control lists) маршрутизатора   
  
Шлюз сеансового уровня:   
Шлюз сеансового уровня (Circuit-level gateway) — межсетевой экран, что исключает прямое взаимодействие между авторизированным клиентом и внешним хостом. Сначала он берет на себя требование уполномоченного клиента на конкретные услуги и, уже после контроля допустимости запрошенного сеанса, определяет соединение с внешним хостом. На рис. 2.2 показано схема функционирование шлюза сеансового уровня.

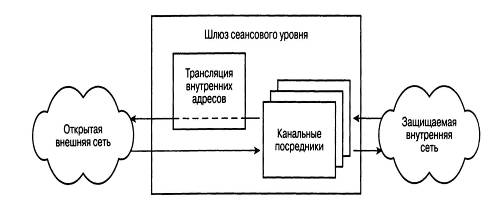


Рис. 2.2. Схема функционирование шлюза сеансового уровня

Уже после предоставленного шлюз попросту копирует пакеты в двух направлениях, никак не исполняя их фильтрации. В этом уровне возникает возможность использования функции общесетевой трансляции адресов (NAT, network address translation). Предоставление внутренних адресов выполняется в соответствии взаимоотношению к совершенно всем пакетам, следующим из внутренней сети в наружную. Для информации пакетов IP-адреса компьютер - отправителей внутренней сети самодействующий преобразуются в один IP-адрес, систематизируемый с защищающим межсетевым экраном. В следствии все без исключения пакеты, идущие с внутренней сети, отправляются межсетевым экраном, что ликвидирует прямой контакт среди внутренней и внешней сети. IP-адрес шлюза сеансового уровня становится одним-единым функционирующим IP-адресом, который поступает в внешнюю сеть.

• Функционирует на 4 уровне

•Сообщает TCP подключения, базируясь в порте

• Приемлемый по цене, но более надежный, чем фильтр пакетов

• Запрашивает активность пользователя или программы конфигурации с целью деятельности

• Пример: SOCKS межсетевой диcплeй

Шлюз прикладного уровня:

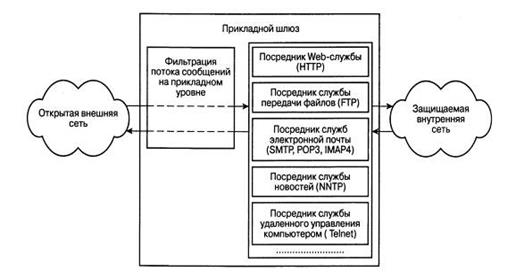
Шлюз прикладного уровня (Application-level gateways) - межсетевой диcплeй, что исключает прямую связь среди автоматизированных клиентом и внешним хостом, фильтруя все без исключения входящие и исходящие пакеты в прикладном уровне модификации OSI. В рис. 2.3 представлено работа шлюза прикладного уровня.

Рис.2.3. Схема функционирование шлюза прикладного уровня

Связанные с приложением программы-посредники перенаправляют через шлюз информацию, генерируемую определенными сервисами TCP/IP.

Возможности:

• Распознавание и аутентификация юзеров при попытке определения соединения посредством межсетевого экрана;

• Фильтрация потока сообщений, например, динамический поиск вирусов;

• Кэширование сведений, запрашиваемых из внешней сети.

На данном уровне возникает возможность применения функций посредничества (Proxy).

С Целью любого обсуживаемого протокола практического уровня, возможно внедрять программных посредников – HTTP-посредник, FTP-посредник и т.д. Посредник любой службы TCP/IP нацелен на обрабатывание уведомлений и выполнение функций защиты, имеющих отношение непосредственно к этой работе. Помимо этого, равно как и шлюз сеансового уровня, практический шлюз перехватывает с поддержкой конкретных защищающих агентов входящие и сходящие пакеты, перенаправляет информацию с помощью шлюза, и функционирует в качестве сервера-посредника, за исключением прямых сочетаний среди внутренней и внешней сети. Однако, посредники, применяемые прикладным шлюзом, обладают значимым отличием с канальных посредников шлюзов сеансового уровня. Посредники прикладного шлюза соединены с определенными приложениями программными серверами), и так же, они имеют все шансы выбирать поток уведомлений на прикладном уровне модификации МВОС.

Характерные Черты:

• Работает на 7 уровне;

• Специфический для приложений;

• Требует деятельность юзера, либо программы конфигурации с целью полной деятельность;

• Пример: Web (http) proxy;

|  |
| --- |
| https://www.bestreferat.ru/images/paper/19/58/7365819.png |

Стек протоколов TCP/IP соотносится с уровнями модели OSI последующим способом:   
Рис. 2.4. Связь уровней стека протоколов ТСР/IР и OSI   
  
Нынешние межсетевые экраны действуют на каждом из упомянутых уровней. На рис. 2.4 представлено взаимосвязь уровней стека протоколов TCP/IP и OSI. Первоначально межсетевые экраны анализировали наименьшее количество уровней; теперь наиболее мощные из них содержат наибольшее количество уровней   
Вне Зависимости от архитектуры межсетевой экран может иметь вспомогательные сервисы. Данные сервисы содержат передачу сетевых адресов (NAT), поддержку протокола динамической конфигурации хоста (DHCP) и функции кодирования.

Многие межсетевые экраны также содержат различные технологии фильтрации активного содержимого. Этот механизм отличается от обыкновенной функции межсетевого экрана тем, то что межсетевой экран теперь также обладает возможностью выбирать настоящие прикладные сведения на уровне 7, которые протекают через него. К Примеру, данный механизм способен быть использован с целью сканирования на предмет присутствия вирусов в файлах, присоединенных к почтовому сообщению.

**2.3 Уровень защищенности межсетевых экранов**

В соответствии с уровнем защищенности межсетевых экранов оценивается по следующим показателям:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
| Наименование показателя | Класс защищенности | | | | | |  |
|  |  |  |  |  |  |  |
| 6 | 5 | 4 | 3 | 2 | 1 |  |
|  |  |
|  |  |  |  |  |  |  |  |
| Дискреционный принцип контроля доступа | + | + | + | = | + | = |  |
|  |  |  |  |  |  |  |  |
| Мандатный принцип контроля доступа | - | - | + | = | = | = |  |
|  |  |  |  |  |  |  |  |
| Очистка памяти | - | + | + | + | = | = |  |
|  |  |  |  |  |  |  |  |
| Изоляция модулей | - | - | + | = | + | = |  |
|  |  |  |  |  |  |  |  |
| Маркировка документов | - | - | + | = | = | = |  |
|  |  |  |  |  |  |  |  |
| Защита ввода и вывода на отчуждаемый физический | - | - | + | = | = | = |  |
| носитель информации |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
| Сопоставление пользователя с устройством | - | - | + | = | = | = |  |
|  |  |  |  |  |  |  |  |
| Идентификация и аутентификация | + | = | + | = | = | = |  |
|  |  |  |  |  |  |  |  |
| Гарантии проектирования | - | + | + | + | + | + |  |
|  |  |  |  |  |  |  |  |
| Регистрация | - | + | + | + | = | = |  |
|  |  |  |  |  |  |  |  |
| Взаимодействие пользователя с КСЗ | - | - | - | + | = | = |  |
|  |  |  |  |  |  |  |  |
| Надежное восстановление | - | - | - | + | = | = |  |
|  |  |  |  |  |  |  |  |
| Целостность КСЗ | - | + | + | + | = | = |  |
|  |  |  |  |  |  |  |  |
| Контроль модификации | - | - | - | - | + | = |  |
|  |  |  |  |  |  |  |  |
| Контроль дистрибуции | - | - | - | - | + | = |  |
|  |  |  |  |  |  |  |  |
| Гарантии архитектуры | - | - | - | - | - | + |  |
|  |  |  |  |  |  |  |  |
| Тестирование | + | + | + | + | + | = |  |
|  |  |  |  |  |  |  |  |
| Руководство для пользователя | + | = | = | = | = | = |  |
|  |  |  |  |  |  |  |  |
| Руководство по КСЗ | + | + | = | + | + | = |  |
|  |  |  |  |  |  |  |  |
| Тестовая документация | + | + | + | + | + | = |  |
|  |  |  |  |  |  |  |  |
| Конструкторская (проектная) документация | + | + | + | + | + | + |  |
|  |  |  |  |  |  |  |  |

Основано на руководящим документе который устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа (НСД) к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997г.

Для каждого класса защищенности определяются требования к указанным показателям.

Далее следуют требования к межсетевому экрану в соответствии с документом Государственной Технической Комиссии по межсетевым экранам для пятого и четвертого класса защищенности и описание уровня соответствия этим требованиям.

**1. Управление доступом.**

Требования к пятому классу:

Межсетевой экран должен обеспечивать фильтрацию на сетевом уровне. Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

Требования к четвертому классу:

Данные требования полностью включают аналогичные требования пятого класса. Дополнительно межсетевой экран должен обеспечивать:

· фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

· фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;

· фильтрацию с учетом любых значимых полей сетевых пакетов.

Требования к третьему классу:

Данные требования полностью включают аналогичные требования четвертого класса.

Дополнительно межсетевой экран должен обеспечивать:

· фильтрацию на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя;

· фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя;

· фильтрацию с учетом даты/времени.

**2. Идентификация и аутентификация**

Нет требований к четвертому и пятому классу. Требования к третьему классу:

Межсетевой экран должен обеспечивать возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

**3. Регистрация**

Нет требований к пятому классу. Требования к четвертому классу:

Межсетевой экран должен обеспечивать возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.

Требования к третьему классу:

Данные требования включают аналогичные требования четвертого класса.

Дополнительно межсетевой экран должен обеспечивать:

· регистрацию и учет запросов на установление виртуальных соединений;

· локальную сигнализацию попыток нарушения правил фильтрации.

**4. Администрирование: идентификация и аутентификация**

Требования к пятому классу:

Межсетевой экран должен обеспечивать идентификацию и аутентификацию администратора межсетевого экрана при его локальных запросах на доступ. Межсетевой экран должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.

Требования к четвертому классу:

Данные требования полностью совпадают с аналогичными требованиями пятого класса.

Требования к третьему классу:

Данные требования включают аналогичные требования пятого класса. Дополнительно межсетевой экран должен препятствовать доступу не идентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась. При удаленных запросах администратора межсетевого экрана на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

**5. Администрирование: регистрация**

Требования к пятому классу:

Межсетевой экран должен обеспечивать регистрацию входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузка и инициализация системы и ее программный останов. Регистрация выхода из системы не проводится в моменты аппаратурного отключения межсетевого экрана;

В параметрах регистрации указываются:

· дата, время и код регистрируемого события;

· результат попытки осуществления регистрируемого события - успешная или неуспешная;

· идентификатор администратора межсетевого экрана, предъявленный при попытке осуществления регистрируемого события.

Требования к четвертому классу:

Данные требования включают аналогичные требования пятого класса.

Дополнительно межсетевой экран должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

Требования к третьему классу:

Данные требования полностью включают аналогичные требования четвертого класса.

Дополнительно межсетевой экран должен обеспечивать регистрацию действия администратора межсетевого экрана по изменению правил фильтрации.

**6. Администрирование: простота использования**

Нет требований к четвертому и пятому классу. Требования к третьему классу:

Многокомпонентный межсетевой экран должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

**7. Целостность**

Требования к пятому классу:

Межсетевой экран должен содержать средства контроля над целостностью своей программной и информационной части.

Требования к четвертому классу:

Данные требования полностью совпадают с аналогичными требованиями пятого класса.

Требования к третьему классу:

Данные требования полностью включают аналогичные требования пятого класса.

Дополнительно должен обеспечиваться контроль целостности программной и информационной части межсетевого экрана по контрольным суммам.

**8. Восстановление**

Требования к пятому классу:

Межсетевой экран должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств межсетевого экрана.

Требования к четвертому классу:

Данные требования полностью совпадают с аналогичными требованиями пятого класса.

Требования к третьему классу:

Данные требования полностью совпадают с аналогичными требованиями пятого класса.

**9. Тестирование**

Требования к пятому классу:

В межсетевом экране должна обеспечиваться возможность регламентного тестирования:

· реализации правил фильтрации;

· процесса идентификации и аутентификации администратора;

· процесса регистрации действий администратора межсетевого экрана;

· процесса контроля за целостностью программной и информационной части межсетевого экрана;

· процедуры восстановления.

Требования к четвертому классу:

В межсетевом экране должна обеспечиваться возможность регламентного тестирования:

· реализации правил фильтрации;

· процесса регистрации;

· процесса идентификации и аутентификации администратора межсетевого экрана;

· процесса регистрации действий администратора межсетевого экрана;

· процесса контроля за целостностью программной и информационной части межсетевого экрана;

· процедуры восстановления.

Требования к третьему классу:

В межсетевое экранирование должна обеспечиваться возможность регламентного тестирования

· реализации правил фильтрации;

· процесса регистрации;

· процесса идентификации и аутентификации запросов;

· процесса идентификации и аутентификации администратора межсетевого экрана;

· процесса регистрации действий администратора межсетевого экрана;

· процесса контроля за целостностью программной и информационной части межсетевого экрана;

· процедуры восстановления.

**10. Руководство администратора защиты**

Требования к пятому классу:

Документ содержит:

· описание контролируемых функций межсетевого экрана;

· руководство по настройке и конфигурированию межсетевого экрана;

· описание старта межсетевого экрана и процедур проверки правильности старта;

· руководство по процедуре восстановления.

Требования к четвертому классу:

Данные требования полностью совпадают с аналогичными требованиями пятого класса.

Требования к третьему классу:

Данные требования полностью совпадают с аналогичными требованиями пятого класса.

**11. Тестовая документация**

Требования к пятому классу:

Должна содержать описание тестов и испытаний, которым подвергался межсетевой экран, и результаты тестирования.

Требования к четвертому классу:

Должна содержать описание тестов и испытаний, которым подвергался межсетевой экран, и результаты тестирования.

Требования к третьему классу:

Должна содержать описание тестов и испытаний, которым подвергался межсетевой экран, и результаты тестирования.

**12. Конструкторская документация**

Требования к пятому классу:

Должна содержать:

· общую схему межсетевого экрана;

· общее описание принципов работы межсетевого экрана;

· описание правил фильтрации;

· описание средств и процесса идентификации и аутентификации;

· описание средств и процесса регистрации;

· описание средств и процесса контроля над целостностью программной и информационной части межсетевого экрана;

Требования к четвертому классу:

Данные требования полностью совпадают с аналогичными требованиями пятого класса по составу документации.

Требования к третьему классу:

Данные требования полностью включают аналогичные требования пятого класса по составу документации.

Дополнительно документация должна содержать:

· описание средств и процесса централизованного управления компонентами межсетевого экрана.

**3. Intrusion Detection Systems (IDS)**

Система обнаружение вторжение:   
IPS системы — это уникальные инструменты, основанные с целью охраны сетей от неавторизованного допуска. Они предполагают из себя аппаратные или компьютерные средства, которые способны незамедлительно выявлять незаконное проникновения. Среди мер, которые принимаются для достижения основных целей IPS, можно отметить оповещение специалистов согласно информационной безопасности, об фактах попыток хакерских атак, а также внедрения вредоносных программ.   
  
Для чего же используют системы обнаружения вторжения в сети?   
Кибератаки — одна из ключевых трудностей, с которыми сталкиваются субъекты, обладающие информационными ресурсами. В том числе известные антивирусные программы и брандмауэры — это средства, которые эффективны только с целью охраны очевидных мест доступа к сетям. Но злоумышленники способны находить пути обхода и уязвимые сервисы в том числе и в наиболее совершенных системах безопасности. При такого рода опасности логично, то что зарубежные и отечественные UTM-решения получают все более широкую известность среди организаций, стремящихся устранить вероятность вторжения и распространения вредоносного ПО. Многочисленные компании получают разрешение приобрести сертифицированный межсетевой экран или иной инструмент с целью комплексной охраны информации.   
  
IDS состоят из 3-х многофункциональных компонентов: информационных источников, анализа и ответа. Система получает сведение о событии из одного или же нескольких источников данных, выполняет определяемый конфигурацией анализ сведений события и потом формирует специализированные решения – от простых отчетов вплоть до активного вмешательства при определении вторжений.   
Выявление вторжения дает возможность организациям защищать собственные системы от угроз, которые объединены с возрастанием сетевой деятельный и важностью информационных систем. При представлении уровня и природы нынешних угроз сетевой безопасности, проблема далеко не в этом, необходимо ли использовать системы выявления проникновений, а в том, какие способности и характерные черты систем обнаружения проникновений необходимо применять.   
  
Почему нужно применять IDS, в особенности если уже существуют межсетевые экраны, противовирусные инструментальные средства и прочие средства защиты?   
  
Межсетевые экраны считаются механизмами создания барьера, преграждая доступ определенным типам сетевого трафика и разрешая другие типы трафика. Формирование такого барьера происходит на основе политики межсетевого экрана. IDS служат механизмами мониторинга, наблюдения активности и принятия решений о том, являются ли наблюдаемые события подозрительными. Они могут выявить атакующих, которые обошли межсетевой экран, а также выдать отчет об этом администратору, который, в свою очередь, предпримет операции по предотвращению атаки.   
IDS становятся важным дополнением инфраструктуры безопасности в любой организации. Технологические Процессы выявления вторжений никак не делают систему совершенно безопасной. Эксплуатация IDS помогает достигнуть нескольких целей:   
1. Возможность иметь реакцию на атаку позволяет заставить атакующего нести ответственность за собственную деятельность.   
2. Возможность блокирования означает возможность определить некоторую активность или событие как атаку и потом осуществить процесс по блокированию источника.  
  
Атакующие, используя легкодоступные технологические процессы, имеют все шансы получить не авторизованный допуск к системам, если найденные в системах уязвимости не исправлены, а сами системы подсоединены к общественным сетям. Объявления о возникновении новых уязвимостей являются общедоступными, к примеру, через публичные сервисы, такие как ICAT или же CERT, которые сформированы с целью того, чтобы эти уязвимости невозможно было применять для выполнения атак. Тем не менее, существует немало ситуаций, в которых применение данных уязвимостей все же допустимо:   
· В многих наследуемых системах не могут быть выполнены все требуемые обновления и модификации.   
· Даже в системах, в которых обновления имеют все шансы быть выполнены, администраторы иногда никак не обладают достаточном количеством времени или ресурсов для отслеживания и инсталлирования абсолютно всех требуемых обновлений. Это является общей проблемой, особенно в окружениях, включающих огромное количество хостов или широкий спектр аппаратуры и ПО.   
· Юзерам могут требоваться функциональности сетевых сервисов и протоколов, которые имеют известные уязвимости.   
· Как пользователи, так и админы совершают погрешности при конфигурировании и применении систем.   
· При конфигурировании системных механизмов управления доступом для реализации определенной политики всегда могут существовать определенные несоответствия. Подобные несоответствия дают возможность законным пользователям осуществлять действия, которые могут причинить ущерб или которые превышают их полномочия.   
3. Возможно определение преамбул атак, как правило имеющих вид сетевого зондирования или некоторого другого тестирования с целью выявления уязвимостей, также предотвращения их дальнейшего формирования. Когда нарушитель атакует систему, он как правило осуществляет определенные предварительные действия. 1-ой стадией атаки как правило считается зондирование или контроль системы. В системах без IDS атакующий беспрепятственно может тщательно исследовать систему с минимальным риском обнаружения. Имея такой неограниченный доступ, атакующий в конечном счете способен отыскать незащищенность и применять ее с целью извлечения нужной информации.   
4. Выполнение документирования существующих опасностей для сети и систем. При составлении отчета о бюджете на сетевую безопасность бывает полезно иметь документированную информацию об атаках. Более того, понимание частоты и характера атак дает возможность принять соответственные меры безопасности.   
5. Обеспечение контроля качества разработки и администрирования безопасности, особенно в крупных и трудных сетях и системах.   
6. Получение полезной информации о вторжениях, которые имели место, с предоставлением улучшенной диагностики для восстановления и корректирования вызвавших проникновение факторов.   
Даже когда IDS не имеет возможности противодействовать атаке, она может составить детальную, достоверную информацию о атаке. Данная информация может находиться в основе соответствующих законодательных мер. В окончательном счете, такая информация может определить проблемы, затрагивающие конфигурации или политики безопасности.   
7. IDS помогает определить расположение источника атак согласно отношению к локальной сети (внешние или внутренние атаки), что важно при принятии решений о расположении ресурсов в сети.

Типы IDS:  
Существует несколько способов классификации IDS, каждый из которых базируется на разных свойствах IDS. Тип IDS следует определять, исходя из следующих характеристик:   
Способ мониторинга системы. По способам мониторинга системы делятся на network-based, host-based и application-based.   
  
Способ анализа. Это часть системы определения вторжения, которая исследует события, полученные из источника данных, и берет на себя решения, что происходит проникновение. Способами анализа считаются выявление злоупотреблений (misuse detection) также выявление аномалий (anomaly detection).   
  
  
  
Развертывание IDS   
Методика выявления вторжений является важным добавлением с целью инфраструктуры общесетевой защищенности во любой огромный компании. Эффективное формирование IDS потребует кропотливого планирования, подготовки, прототипирования, испытания также особого преподавания.   
Необходимо основательно подбирать стратегию выявления вторжения, консистентную со общесетевой инфраструктурой, политикой защищенности также существующими ресурсами.   
  
Стратегия развертывания IDS   
Необходимо определить несколько стадий развертывания IDS, для того чтобы персонал имел возможность получить опыт и сформировать необходимый мониторинг и нужное количество ресурсов в целях функционирования IDS. Необходимые ресурсы для каждого типа IDS могут отличаться, в частности, и в зависимости от системного окружения. Следует иметь соответствующую политику безопасности, планы и процедуры, для того чтобы персонал располагать сведениями, как обрабатывать многочисленные сигналы тревоги, выдаваемые IDS.   
С Целью защиты сети предприятия рекомендуется проанализировать комбинацию network-based IDS и host-based IDS. Далее необходимо установить стадии развертывания, начиная с network-based IDS, так как они обычно являются наиболее легкими для инсталлирования и сопровождения. Уже после этого необходимо защитить критичные серверы с помощью host-based IDS. Применяя инструментальные ресурсы анализа уязвимостей, необходимо испытать IDS и другие механизмы безопасности относительно правильного конфигурирования и функционирования.   
  
Подобные технологические процессы, как Honey Pot, должны применяться только лишь в том случае, если есть достаточная техническая квалификация администратора.   
  
Развертывание network-based IDS   
Единственный вопрос, который необходимо внимательно продумать при развертывании network-based IDS, — это размещение системных сенсоров. Имеется большое количество вариантов расположения network-based IDS, каждый из которых имеет свои преимущества:   
1. Основная подсеть   
2. Подсеть с критичными ресурсами и дополнительными точками доступа   
3. DMZ-сеть

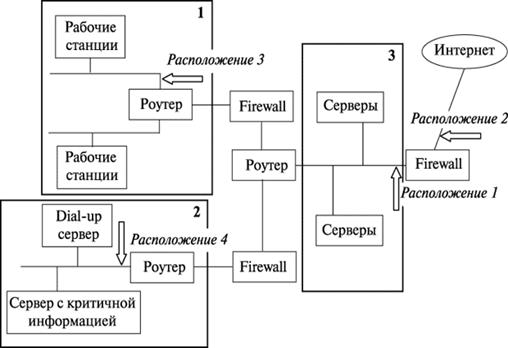


Рис. 3.1. Возможные варианты расположения сенсоров network-based IDS   
Позади внешнего межсетевого экрана в DMZ-сети (расположение 1)   
  
Преимущества:   
· Видит атаки, исходящие из наружного мира, которым удалось преодолеть первую линию обороны сетевого периметра.   
· Способен анализировать проблемы, которые связаны с политикой или производительностью межсетевого экрана, который обеспечивают главную линию обороны.   
· Видит атаки, целями которых являются прикладные серверы, как правило расположенные в DMZ.   
· Даже в случае если входящая атака никак не распознана, IDS иногда способен определить исходящий трафик, который возникает в результате компрометации сервера.   
  
Перед внешним межсетевым экраном (расположение 2)   
  
Преимущества:

· Документирует количество атак, исходящих из Интернета, целью которых является сеть.   
  
· Документирует разновидности атак, исходящих из Интернета, целью которых является сеть.

В основной магистральной сети (расположение 3)

Преимущества:   
  
· Просматривает основной сетевой трафик; тем самым возрастает вероятность распознания атак.   
  
· Определяет неавторизованную деятельность авторизованных пользователей внутри периметра безопасности организации.   
  
В критичных подсетях (расположение 4)   
  
Преимущества:   
  
· Определяет атаки, целью которых считаются критичные системы и ресурсы.   
  
· Дает Возможность сосредотачиваться на ограниченных ресурсах наиболее важных информационных ценностей, находящихся в сети.   
  
Развертывание host-based IDS   
  
После того как network-based IDS размещены и функционируют, с целью повышения степени защиты системы дополнительно может быть рассмотрено применение host-based IDS. Однако инсталлирование host-based IDS в любой хост может потребовать значительных временных затрат. По Этой Причине рекомендовано, для того чтобы в первую очередь host-based IDS были инсталлированы на критичных серверах. Это может сократить общую стоимость развертывания и даст возможность основное внимание уделить реагированию на тревоги, касающиеся более значимых хостов. После того как host-based IDS начали функционировать в обычном режиме, организации с высокими требованиями к безопасности могут обсудить возможность инсталлирования host-based IDS на другие хосты. В этом случае следует приобретать host-based системы, которые имеют централизованное управление и функции формирования отчетов. Подобные возможности могут значительно уменьшить сложность управления сообщениями об тревогах от большого числа хостов.   
  
Далее следует рассмотреть возможность увеличения квалификации администраторов. В большинстве случаев результативность конкретной host-based IDS зависит от способности администратора распознавать ложные и верные тревоги.

Стратегии оповещения о тревогах   
  
Наконец, при развертывании IDS важной проблемой считается установление того, какие непосредственно возможности оповещения IDS о тревогах использовать в каждом определенном случае. Большая часть IDS поставляются с уже сконфигурированными возможностями уведомления о тревогах, которые имеют широкий спектр опций, включая посылку уведомлений на e-mail, использование протоколов сетевого управления и автоматическое блокирование источника атаки.

**3.1 IPv6 как сильное влияние на конструкцию межсетевого экрана**

Из всех новшеств, которые появились в ближайшие несколько лет, наибольшее влияние на конструкцию межсетевых экранов окажет одно - новое поколение протокола IP.   
IPv6 сможет взаимодействовать с IPv4, и точнее всего развертывание IPv6 произойдет путем плавной смены, в процессе которой оба протокола будут мирно сосуществовать.   
  
Совместная работа IPv4 и IPv6   
Как будет обеспечиваться возможность коллективной работы IPv4 и IPv6 в одной сети? В настоящий момент для этого предлагается 2 метода. Первый из них заключается в применении в системах с IPv6 2-ух различных стеков протоколов, 1-го для IPv4, а другого для IPv6. Их выбор будет определяться видом протокола, используемого на узле, с которым устанавливается соединение. 2-Ой способ заключается в туннелировании пакетов IPv6 внутри пакетов IPv4 при размене данными между ПК с IPv6 по маршруту, включающему ПК с IPv4.   
  
Заголовок IPv6   
Протяженность нового заголовка IP-пакета равна 40 байтам. Благодаря тому, что эта величина фиксирована, сетевые устройства смогут обрабатывать пакеты гораздо быстрее. На рис. 3.2 видно, что новый заголовок имеет меньше полей, нежели заголовок IPv4.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Версия | Класс трафика | Метка потока | | |
| Длина данных | | | Следующий заголовок | Счетчик сегментов |
| Адрес отправителя | | | | |
| Адрес получателя | | | | |

Рис. 3.2. Длина заголовка IPv6 фиксирована и равна Сорок б   
  
Следующие поля заголовка IPv4 были исключены из заголовка IPv6:   
· поля, относящиеся к фрагментации, подобные как Fragment Offset (Смещение фрагмента) и Identification (Идентификатор), а также флаги Don\'t Fragment (Запрет фрагментации) и More Fragments (Флаг фрагментации);   
· поле контрольной суммы;   
· поле параметров.   
  
С Целью повышения скорости обрабатывания пакетов в IPv6 было принято решение отказаться от их фрагментации. Очередной маршрутизатор, никак не способен передать дальше слишком огромный пакет, не станет разбивать его на части, которые придется собирать на принимающем конце. Вместо данного пакет будет отброшен, а маршрутизатор возвратит новое сообщение ICMP (Packet Too Big - слишком большой размер пакета) отправителю, который сумеет независимо разделить сообщение на более мелкие пакеты.   
  
Последующей попыткой увеличить скорость обрабатывания пакетов в IPv6 является отказ от поля контрольной суммы пакета. Каждый маршрутизатор на пути пакета должен заново определять роль данного поля, таким образом, как счетчик сегментов в поле TTL снижается в любом новейшем узле. Так как ревизорская совокупность рассчитывается во лежащем в основе IP канальном уровне, а также в протоколах TCP и UDP, удаление данного поля с IP-заголовка никак не спровоцирует никаких проблем.   
  
Новые сообщения ICMP   
  
Протокол IP с поддержкой сообщений ICMP осуществляет множество функций, наиболее известной из которых считается проверка доступности узла удаленной сети утилитой PING, что отправляет для данного эхо информацию ICMP. Как и протокол IP, ICMP будет расширен, для того чтобы идти в ногу со временем. Помимо перемен, связанных с внедрением IPv6, в ICMP будут включены функции протокола Internet Group Management Protocol (IGMP, протокола управления группами Internet).   
  
С полем Options (Параметры) положение другое. Это поле переменной длины было убрано из IP-заголовка, для того чтобы его длина оказалась фиксированной, но это не обозначает, что удалены также и характеристики. Они могут быть заданы в поле Next Header (Следующий протокол), которое обычно обозначает другой протокол, такой как TCP или UDP. В данном случае характеристики помещаются в область данных пакета, а в поле Next Header находится указатель их положения. Из-За отсутствия параметров в заголовке пакет IP-пакеты обрабатываются значительно стремительнее.   
  
В новом заголовок IPv6 могут содержаться следующие поля:   
  
· Version (Версия) - 4-битное поле, означающее, как и в IPv4, версию протокола IP. В IPv6 постоянно имеет значение 6;   
  
· Traffic Class (Класс трафика) - 8-битное поле, специализированно для тех же целей, что и поле Type of Service (Тип службы) в заголовке IPv4;   
  
· Flow Label (Метка потока) - применяется с целью обозначения различных потоков (flows) трафика. Позволяет задавать приоритеты обработки потоков. Конечного определения потока еще нет. Это может быть наиболее дорогостоящий трафик, или трафик с аудио- или видеоданными;   
  
· Payload Length (Длина данных) - 16-битное поле, показывающее число байт в блоке данных, который идет после заголовка;   
  
· Next Header (Следующий заголовок) - предназначается для установления протокола наиболее высочайшего уровня, которому IP транслирует пакет с целью последующей обрабатывания. В данном поле используются те же номера протоколов, что и в IPv4;   
  
· Hop Limit (Счетчик сегментов) - максимально допустимое количество сегментов. Любой маршрутизатор, через который идет пакет, уменьшает значение данного поля на единицу. Если значение счетчика становится равным нулю, пакет отбрасывается;   
  
· Source Address (Адрес отправителя) — 128-битное поле с адресом отправителя пакета;   
  
· Destination Address (Адрес получателя) - 128-битное поле с адресом получателя пакета.   
  
Расширенные заголовки   
  
Поле Next Header в 40-байтном заголовке зафиксированной длины предназначается с целью обозначения вида заголовка, который будет находится в истоке области данных IP-пакета. Вспомним, что внутри пакета IP как правило располагается пакеты протокола наиболее высочайшего уровня, такого как TCP или UDP, который имеет индивидуальный заголовок. За счет использования IP-заголовка фиксированной длины обрабатывание пакетов на маршрутизаторах и других сетевых аппаратах намного ускоряется. Однако так как некоторые поля были исключены из заголовка, для выполнения их функций должны быть учтены другие методы.   
  
По Этой Причине было создано ряд типов так называемых расширенных заголовков (extension headers), которые кроме того могут находиться в истоке области данных IP-пакета. При данном поле Next Header указывает на углубленный заголовок. В качестве подобных заголовков допускается указывать следующие:   
  
· Hop-by-Hop Options (Параметры, проверяемые на каждом узле);   
  
· Fragmentation (Фрагментация);   
  
· Routing (Маршрутизация);   
  
· Authentication (Аутентификация);   
  
· Security Encapsulation (Защита содержания);   
  
· Encapsulation Security Payload (Безопасное закрытие содержания);   
  
· Destination Options (Параметры получателя).

Адресация IPv6   
При переходе от 32 бит к 128 битам адресное пространство IPv6 астрономически возрастет согласно сопоставлению с IPv4.   
  
В IPv6 имеется 3 ключевых типа адресов:   
  
· unicast (индивидуальный) - оригинальный личный номер конкретного сетевого интерфейса;   
  
· anycast (любой) - обозначает ряд интерфейсов. Пакет, ориентированный на адрес типа anycast, будет передан на ближайший интерфейс (определенный используемым протоколом маршрутизации), заданный данным адресом;   
  
· multicast (групповой) - также указывает на ряд интерфейсов. Однако в отличие от варианта с адресом типа anycast, пакет, направленный на адрес типа multicast, пересылается абсолютно всем интерфейсам, обозначенным этим адресом.   
  
Несмотря на то, что адрес типа unicast считается неповторимым идентификатором сетевого интерфейса, один интерфейс может иметь несколько unicast-адресов. Широковещательных (broadcast) адресов больше нет - их функциональность унаследовал тип адресов multicast.

**Заключения**

Ознакомившись с описанными трудностями, можно сделать заключение, то что межсетевые экраны гарантируют охрану компьютерной сети компании от несанкционированного вмешательства. Межсетевые экраны считаются важным средством обеспечения информационной безопасности. Они гарантируют максимальную линию обороны. При подборе и приобретении межсетевых экранов необходимо основательно все проанализировать. Подобрать подходящую архитектуру и компонентов межсетевого экрана. Грамотно настроить программную обеспечению также проводить тестирование конфигурации межсетевого экрана.

**Список сокращений и обозначений**

|  |  |
| --- | --- |
| КСО | Компьютерный сеть организации |
| ИБ | Информационная безопасность |
| ОС | Операционная Система |
| ПО | Программное Обеспечение |
| НСД | Несанкционированный доступ |
| СОИБ | Система обеспечения информационной безопасности |
| СУБД | Система управлением база данных |
| ЦП | Центральный Процессор |
| CA | Certification Authority |
| CGI | Common Gateway Interface |
| DHCP | Dynamic Host Configuration Protocol |
| DMZ | Demilitarized Zone |
| DNS | Domain Name System |
| DoS | Denial of Service |
| DSA | Digital Signature Algorithm |
| FTP | File Transport Protocol |
| GUI | Graphical User Interface |
| HTML | Hyper Text Markup Language |
| HTTP | Hyper Text Transfer Protocol |
| IDS | Intrusion Detection System |
| IIS | Internet Information Services |
| KSK | Key Signing Key |
| MAC | Media Access Control |
| MAC | Message Authentication Code |
| MD5 | Message Digest v5 |
| NAT | Network Address Translation |
| NTP | Network Time Protocol |
| NTP | Network Time Protocol |
| OSI | Open System Interconnection |
| PKI | Public Key Infrastructure |
| RSA | Rivest, Shamir, Adleman |
| SEP | Secure Entry Point |
| SHA | Secure Hash Algorithm |
| SMTP | Simple Mail Transfer Protocol |
| SSH | Secure Shell |
| SSL | Secure Socket Layer |
| TOS | Trusted ОС |
| VPN | Virtual Private Network |
| URL | Uniform Resource Locator |
| REP | Robots Exclusion Standard |
| IE | Internet Explorer |
| SSI | Server Side Includes |
| ASP | Active Server Pages |
| ISP | Internet Service Provider |

**Список использованных источников литературы**

1. О.Р. Лапонина. Межсетевое экранирование. «ИНТУИТ», М., 2009;

2. Е. Баранова, А. Бабаш. Информационная безопасность и защита информации. 3-е изд. М. 2016.;

3. Девид Чемпен, Энди Фокс. Брандмауэры Cisco Secure PIX. «Вильямс», М., 2009;

4. А. Бирюков. Информационная безопасность: защита и нападение. 2-е изд. М. 2017.;

5. А.Ю. Щеглов. Защита компьютерной сети от несанкционированного доступа. «НиТ», Спб., 2009;

6. В. Бондарев. Введение в информационную безопасность автоматизированных систем. М. 2016.;

7. Михеева Е.В. Информационные технологии в профессиональной деятельности: учебное пособие. – М.: Проспект, 2010.

**Интернет ресурсы**

1. https://fstec.ru

2. http://www.consultant.ru/

3. http://www.consultant.ru/

4. http://opennet.ru

5. http://infosecurity.ru

6. http://osp.ru

7. http://www.oszone.ru