Содержание:

Введение

Информационные технологии в современном мире постоянно претерпевают изменения, которые направлены на множество аспектов, связанных с жизнью и деятельностью людей и организаций. Изменению подвержены способы хранения, обработки и передачи информации, благодаря этому, качественно изменяются возможности использования информации и результатов ее анализа и обработки. Информационные ресурсы приобретают свойства значительного масштабирования в рамках территориально распределенных информационных систем. Технологии позволяют людям и организациям постоянно иметь доступы к необходимым для них информационным ресурсам, где бы они (люди, организации или ресурсы) не находились, при этом информация остается надежно защищенной от несанкционированного доступа, модификации или уничтожения.

Благодаря современным технологиям защиты информации многие организации формируют свою стратегию в области информационных технологий учитывая возможности Интернета, как одного из основных механизмов передачи информации, в том числе и той, которая является конфиденциальной для организации. В этой связи, при проектировании сетевой инфраструктуры организации, одним из важнейших этапов проектирования является выбор технологии защищенного доступа из Глобальной сети Интернет к ресурсам и сервисам локальной сети организации.

В настоящее время существует несколько распространенных технологий защищенного доступа к локальным сетям организаций через сеть Интернет. Несмотря на то, что все технологии защищенного доступа базируются на одних и тех же фундаментальных механизмах построения глобальных и локальных сетей, в зависимости от цели доступа, могут использоваться разные варианты реализации технологий защищенного доступа. Локальные вычислительные сети организаций в своем составе помимо информационных ресурсов могут содержать информационные сервисы. При проектировании механизмов, защищающих локальные сети организаций от несанкционированного вторжения и возможных атак на конфиденциальность и целостность информации, это необходимо

учитывать.

В настоящей работе будут рассмотрены основные понятия обеспечения информационной безопасности локальный сетей организаций, современные аппаратные и программные решения, позволяющие организовать защищенный доступ к локальным сетям организаций. Так же будет проведен анализ указанных решений на наличие в них сильных и слабых сторон с точки зрения эффективности защиты локальных сетей.

На примере организации «МИРАН» будет спроектирована система защищенного доступа к локальной сети этой организации через сеть Интернет. В курсовой работе будет проанализирована специфика деятельности, информационные ресурсы и сервисы организации «МИРАН». Система защищенного доступа к локальной сети организации будет учитывать особенности данной организации.

Практическая значимость работы заключается в создании возможности использования полученных результатов для выбора технологий и реализации защищённых систем доступа к локальным сетям организаций.

Работа включает в себя две главы: аналитическую и практическую части:

- В аналитической части будет рассмотрены вопросы обеспечения информационной безопасности локальных сетей предприятия, анализ современных технологий защищенного доступа к сетям, будет проведена декомпозиция задачи построения системы защищенного доступа к локальной сети организации «МИРАН»;
- В практической части работы будет организация «МИРАН» будет проанализирована на предмет наличия и специфики элементов в локальной сети, к которым необходимо предоставить защищенный доступ из сети Интернет. На основе анализа будут выбраны необходимые технологии и спроектирована система защищенного доступа к локальной сети организации.

Глава 1. Аналитическая часть

Глобальная сеть интернет является общедоступной. Именно по этой причине она стала одним из основных механизмов обмена информацией между людьми и организациями. Но, так же по причине общей доступности, Интернет для локальных сетей организаций несет существенные угрозы информационной

безопасности. Для локальных сетей организация современные сетевые технологии могут нести следующие угрозы:

- Угрозы конфиденциальности информации;
- Угрозы целостности информации;
- Угрозы доступности к данным или средствам управления информационными сервисами;

Вероятность реализации той или иной угрозы повышается если организация использует в своей сетевой инфраструктуре механизмы удаленного доступа пользователей через Интернет. Но грамотно спроектированная и реализованная система информационной безопасности позволяет компенсировать повышение вероятности реализации угрозы.

Основные понятия обеспечения информационной безопасности локальных сетей предприятий

Информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Это понятие «информационного ресурса», сформулированное в федеральном законе № 24 ФЗ «Об информатизации и защите информации» от 20.02.1995 г. Современная трактовка термина «информационный ресурс» организации является очень похожей – это те же массивы данных, являющиеся собственностью организации. В информационных ресурсах находиться информация, которой организация руководствуется в своей работе или которую организация генерирует, как результат своей работы. Процессы или механизмы доступа к такой информации для работы с этой информацией называются «информационными сервисами».

Информационная безопасность в организации – это процесс, результатом работы которого является обеспечение доступности, целостности и конфиденциальности информации, находящейся в информационных ресурсах локальной сети организации. Под доступностью информации необходимо понимать именно доступность, возможность информацией воспользоваться. Целостность информации – это обеспечение достоверности информации и гарантии того, что информация не модифицирована. Конфиденциальность информации – это

обеспечение доступности только тем пользователям, у которых есть на это право.

Угроза информационной безопасности организации – это вероятная возможность различными способами нарушить информационную безопасность. Например, вызвать отказ в доступе к информации или информационным ресурсам авторизованным пользователям, исказить информацию, нарушив ее целостность, предоставить доступ к ресурсам сети пользователям, не имеющим необходимых полномочий в сети. Попытка реализации угрозы информационной безопасности – это атака на ресурсы или сервисы локальной сети. Классификация видов угроз информационной безопасности представлена на рисунке 1.

Рисунок 1. Классификация видов угроз информационной безопасности

Как видно из рисунка 1, при реализации удаленного доступа к локальной сети предприятия могут быть созданы предпосылки к реализации угроз информационной безопасности:

- Доступность и конфиденциальность информации – при ошибках в выборе технологий и в конфигурировании систем защиты каналов удаленного доступа;
- Реализованная угроза конфиденциальности информации провоцирует повышение вероятности реализации угрозы целостности информации.

Для обеспечения информационной безопасности в локальных сетях организации могут выполнятся следующие мероприятия (по категориям):

- Организационные
  - Административные меры. К таким мерам относят подготовку и выполнение планов по реализации информационной безопасности в организации;
  - Процедурные меры. Данные меры ориентированы на людей, формирующих режим информационной безопасности в организации, и создающих «Человеческий фактор», провоцирующий нарушение созданного режима. Данные меры включают в себя обязательную реакцию на инциденты, связанные с нарушением режима информационной безопаности;
  - Физическая защита информации: грамотная поддержка пользователей, поддержка программного обеспечения, резервное копирование, документирование.
- Технические:
  - Идентификация и аутентификация – это основные программно-технические средства информационной безопасности, направленные на защиту именованных ресурсов и сервисов. Эти средства позволяют установить доверительные отношения между владельцами и потребителями информационных ресурсов и сервисов. Данная группа технических мероприятий предусматривает: парольную защиту, одноразовые пароли, идентификацию при помощи биометрических данных,
  - Управление доступом – средства управления доступом позволяют специфицировать и контролировать действия, которые пользователи и процессы могут выполнять над информацией и другими компьютерными ресурсам. В данном разделе речь идет о логическом управлении доступом, которое, в отличие от физического, реализуется программными средствами. Логическое управление доступом - это основной механизм многопользовательских систем, призванный обеспечить конфиденциальность и целостность объектов и, до некоторой степени, их доступность. [2]
  - Протоколирование и аудит – это сбор, накопление и анализ данных о событиях, происходящих в локальной сети, информационных системах. Накопленная информация проходит анализ для выявления потенциально опасных действий пользователей. Такой анализ называется Аудитом.

- Шифрование – это наиболее действенное мероприятия для обеспечения конфиденциальности информации. Это мероприятие во многих случаях занимает центральное место среди программно-технических комплексов, обеспечивающих информационную безопасность.
- Контроль целостности – в данном мероприятии применяются криптографические методы контроля целостности передаваемого информационного потока. В основе данного контроля лежит понятие хеш-функции и электронно-цифровой подписи.
- Экранирование – это техническое мероприятия, с использованием которого уменьшается уязвимость внутренних мер безопасности, поскольку первоначально злоумышленник должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно. Кроме того, экранирующая система, в отличие от универсальной, может быть устроена более простым и, следовательно, более безопасным образом. Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима конфиденциальности в ИС организации. [3]
- Анализ защищенности – мероприятие, предназначенное для выявления уязвимых мест с целью их оперативной ликвидации. Сам по себе этот сервис ни от чего не защищает, но помогает обнаружить пробелы в защите раньше, чем их сможет использовать злоумышленник. В первую очередь, имеются в виду не архитектурные, а бреши, появившиеся в результате ошибок администрирования или из-за невнимания к обновлению версий программного обеспечения. Системы анализа защищенности, как и рассмотренные выше средства активного аудита, основаны на накоплении и использовании знаний. В данном случае имеются в виду знания о пробелах в защите: о том, как их искать, насколько они серьезны и как их устранять. Соответственно, ядром таких систем является база уязвимых мест, которая определяет доступный диапазон возможностей и требует практически постоянной актуализации.
- Туннелирование – это мероприятие, представляющее собой самостоятельную меру безопасности. Оно заключается в упаковке информационных пакетов таким образом, чтобы обеспечить конфиденциальность и целостность передаваемых данных при использовании вместе с криптографическими методами защиты.

- Правовые – данные меры в основном направлены на регулирование действий в области защиты информации посредством нормативно-правовых и нормативно-методических документов, разрабатываемых на разных уровнях: международном, государственном, локальном. В настоящей работе правовые мероприятия, способствующие реализации системы информационной безопасности, рассматриваться не будут.

При проектировании локальных сетей организаций, при проектировании доступов к ресурсам и сервисам локальных сетей из Интернета, применяются все вышеперечисленные мероприятия. Рассмотрим более подробно технологии, позволяющие организовать защищенный доступ к локальной сети.

Анализ современных технологий защищенного доступа к локальным сетям организаций из сети Интернет

В качестве примера рассмотрим локальную сеть со следующими сервисами и ресурсами:

- Корпоративный почтовый сервер (web-mail);
- Корпоративный терминальный сервер (RDP);
- Сервер, поддерживающий сервис для клиентов (Web-API) для считывания текущего состояния заказа клиента;
- Сеть построена на контроллере домена Active Directory;
- В сети находиться корпоративное программное обеспечение SAP ERP.

Локальная сеть в составе аппаратного обеспечения может использовать маршрутизаторы Cisco ISR 400 и межсетевой экран Juniper Networks NetScreen 5200.

Рассмотрению подлежат следующие варианты защищенного удаленного доступа через сеть Интернет:

- Плоская сеть;
- Создание демилитаризованной зоны;
- Разделение сервисов на Front-End и Back-End;
- Создание защищенного доступа в корпоративную сеть посредством реализации VPN с аутентификацией в Active Directory;

Реализация защищенного доступа к локальной сети организации по варианту «Плоская сеть» (Рисунок 2).

При реализации варианта Плоская сеть, все узлы и хосты организации находятся в одной общей сети (внутренняя сеть). В рамках внутренней сети коммуникации между узлами и хостами не ограничиваются. Локальной сеть подключена к сети Интернет посредством пограничного маршрутизатора или маршрутизатора доступа. Внутренняя сеть находиться под управлением контроллера домена.

Доступ узлов и хостов локальной сети организации в сеть Интернет осуществляется посредством механизма преобразования сетевых IP-адресов транзитных пакетов (NAT). Данный механизм работает следующим образом: Принимая пакет от хоста внутренней сети маршрутизатор проводит контроль IP-адреса назначения. Если IP-адрес принадлежит внутренней сети, то пакет пересылается внутреннему хосту, иначе пакет пересылается в Интернет, при этом, чтобы предупредить недоступность невидимого из Интернета хоста-отправителя, маршрутизатор подменяет обратный IP-адрес на свой внешний, видимый из Интернета IP-адрес. Для сортировки ответных пакетов, которые адресованы разным внутренним хостам, маршрутизатор, помимо подмены IP-адреса, меняет номер порта. Все подмены IP-адресов и номеров портов хранятся во временной таблице маршрутизатора.

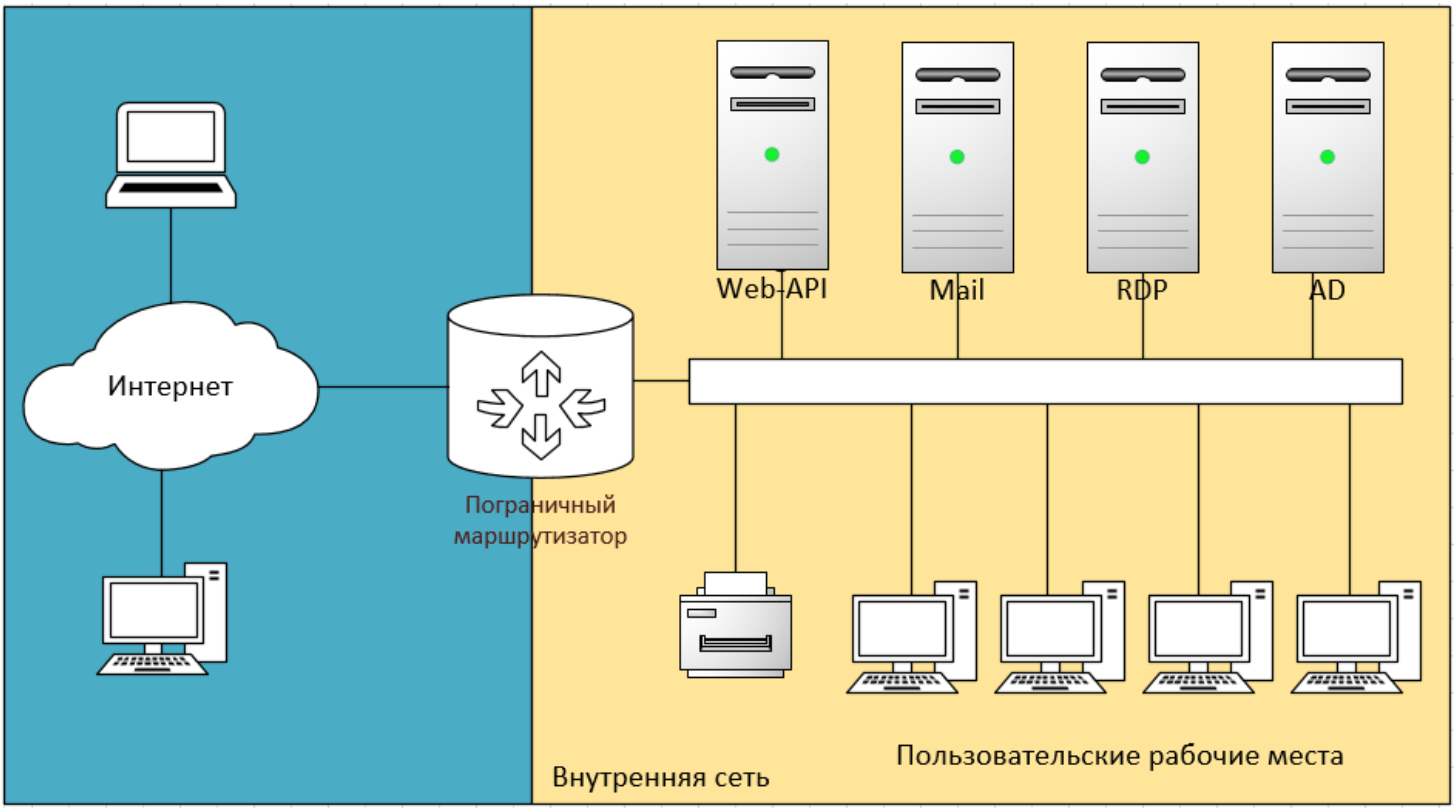

Рисунок 2. Схема удаленного доступа к локальной сети из интернета по варианту «Плоская сеть»

Доступ к ресурсам и сервисам локальной сети организации из сети Интернет осуществляется посредством технологии Port Forwarding, которая позволяет получить доступ к хосту или сервису в локальной сети с пограничным маршрутизатором NAT. Доступ реализуется при помощи перенаправления трафика от строго определенных портов с внешнего IP-адреса пограничного маршрутизатора на IP-адрес хоста локальной сети.

Доступ к любым ресурсам сети возможен через комбинацию AD и RDP.

Вариант «Плоская сеть» является, по сравнению с другими, наиболее простым в реализации и наименее затратным по стоимости оборудования и специалистов.

Плюсы варианта:

- Крайне низкие требования к аппаратному обеспечению. Технологиями NAT и Port Forwarding оснащены все современные маршрутизаторы (в том числе и для домашнего использования).
- Требования к компетенциям сетевых инженеров не высокие. Современные устройства в большинстве случаев имеют удобные пользовательские интерфейсы для настройки доступов.

Минусы варианта:

- Данная технология обеспечивает минимальный уровень безопасности. При взломе хотя бы одного сервера с получением к нему доступа, злоумышленник может получить возможности несанкционированного доступа ко всем хостам локальной сети.

Реализация защищенного доступа к локальной сети организации по варианту «Создание демилитаризованной зоны» (Рисунок 3).

Очевидным недостатком реализации защищенного доступа к локальной сети организации через Интернет по варианту Плоская сеть являлась низкая степень безопасности реализации. Вариант «Создание демилитаризованной зоны» позволяет физически сформировать сегменты сети: «Демилитаризованная зона» в которой находятся сервера, сервисы которых опубликованы в Интернете и «Внутренняя сеть». Сегмент «Демилитаризованная зона» формируется посредством межсетевых экранов, которые отделяют сегмент от Интернета и

Внутренней сети.

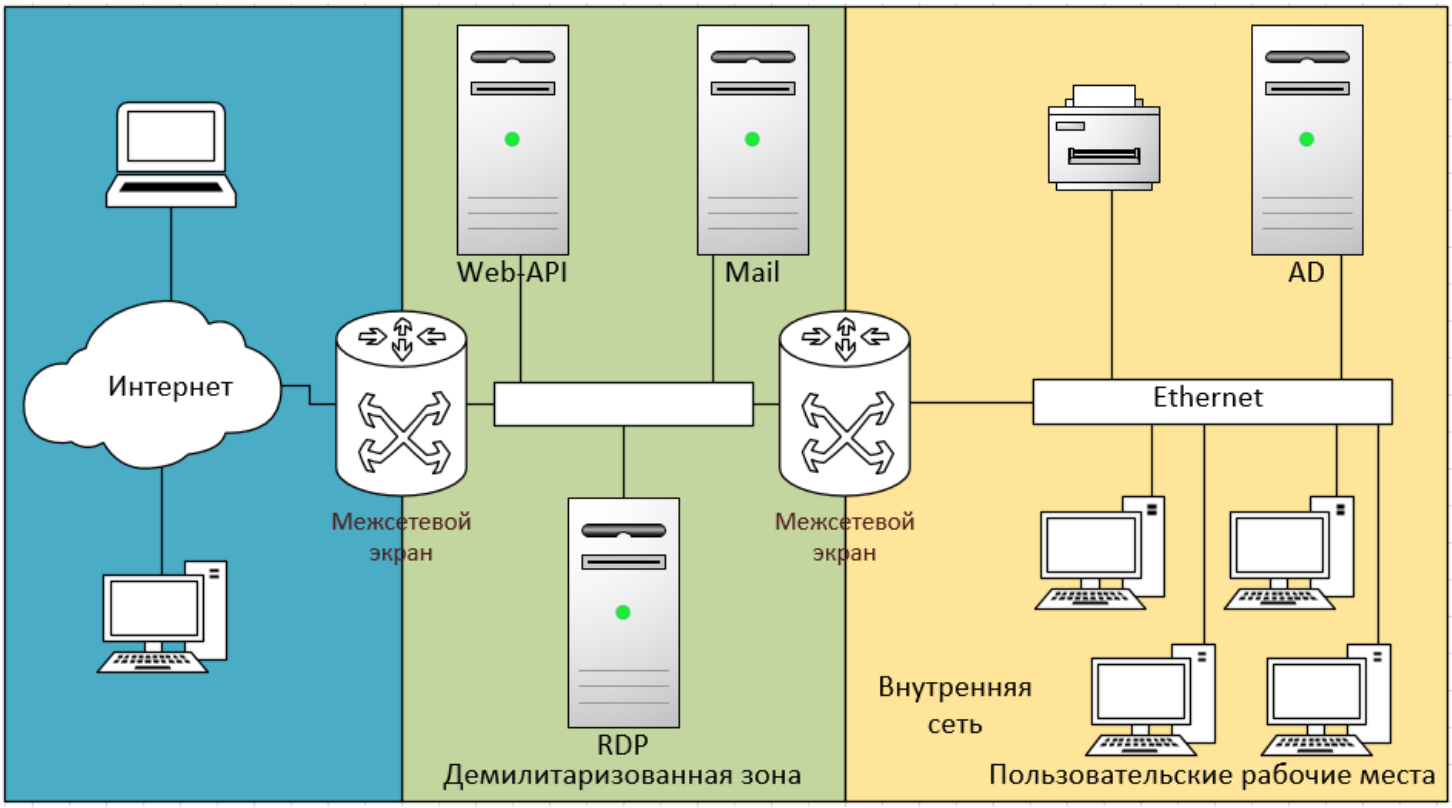

Рисунок 3. Схема удаленного доступа к локальной сети из интернета по варианту «Создание демилитаризованной зоны»

При реализации данного варианта важнейшим этапом является конфигурирование правил фильтрации IP-пакетов на межсетевых экранах. В общем эти правило могут быть сформированы следующим образом (Рисунок 4):

- Из внутренней сети можно инициировать соединение в демилитаризованную зону и глобальную сеть (Интернет);
- Из демилитаризованной зоны можно инициировать соединение в глобальную сеть (Интернет);
- Из глобальной сети (Интернет) можно инициировать соединение в демилитаризованную зону;
- Нельзя инициировать соединение во внутреннюю сеть из Глобальной сети (Интернет) и из демилитаризованной зоны.

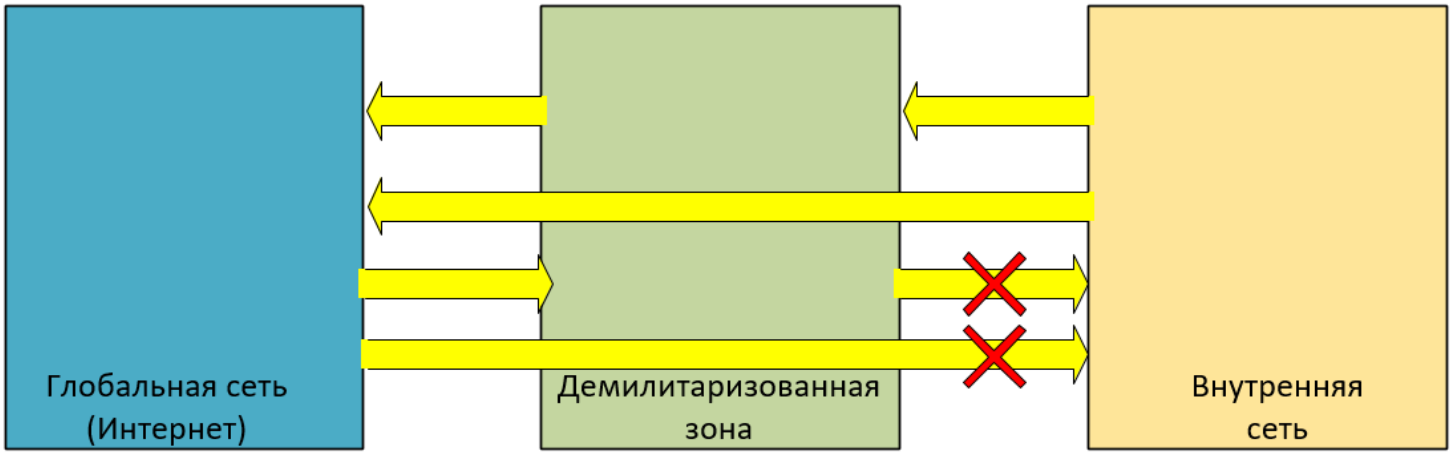

Рисунок 4. Правила конфигурировать фильтрации пакетов на сетевых экранах при реализации варианта «Создание демилитаризованной зоны»

Плюсы варианта:

- Реализация варианта «Создание демилитаризованной зоны» позволяет существенно повысить степень защищенности внутренней сети от взломов через отдельные сервисы. Благодаря межсетевому экрану во внутреннюю сеть доступ к ресурсам внутренней сети не будет получен.

Минусы варианта:

- Сервера, находящиеся в демилитаризованной зоне имеют не высокую степень защищенности от взлома.
- Необходим дополнительный аппаратный межсетевой экран для разделения демилитаризованной зоны и внутренней сети.

Для повышения степени защищенности серверов, находящихся в демилитаризованной зоне, необходимо применять политики безопасности на оборудовании отличные от настроенных по умолчанию производителем оборудования.

Реализация защищенного доступа к локальной сети организации по варианту «Разделение сервисов на Front-End и Back-End».

Вариант с Демилитаризованной зоной несет существенную угрозу информационной безопасности организации в части повышения рисков отказа доступа к информации. Ото обусловлено низкой защищенностью самой демилитаризованной зоны. Действенным способом решения данной задачи является разделение функционала сервиса на Front-End и Back-End части. При этом каждая часть должна

быть расположена на отдельном сервере в своем сегменте сети. Front-End часть сервиса, которая отвечает за взаимодействие с клиентами и удаленными сотрудниками размещается на сервере в демилитаризованной зоне. Back-End часть сервиса, отвечающая за реализацию основного функционала сервиса (работа с базами данных, обработка информации и т.д.) размещается на сервере во внутренней сети (Рисунок 5).

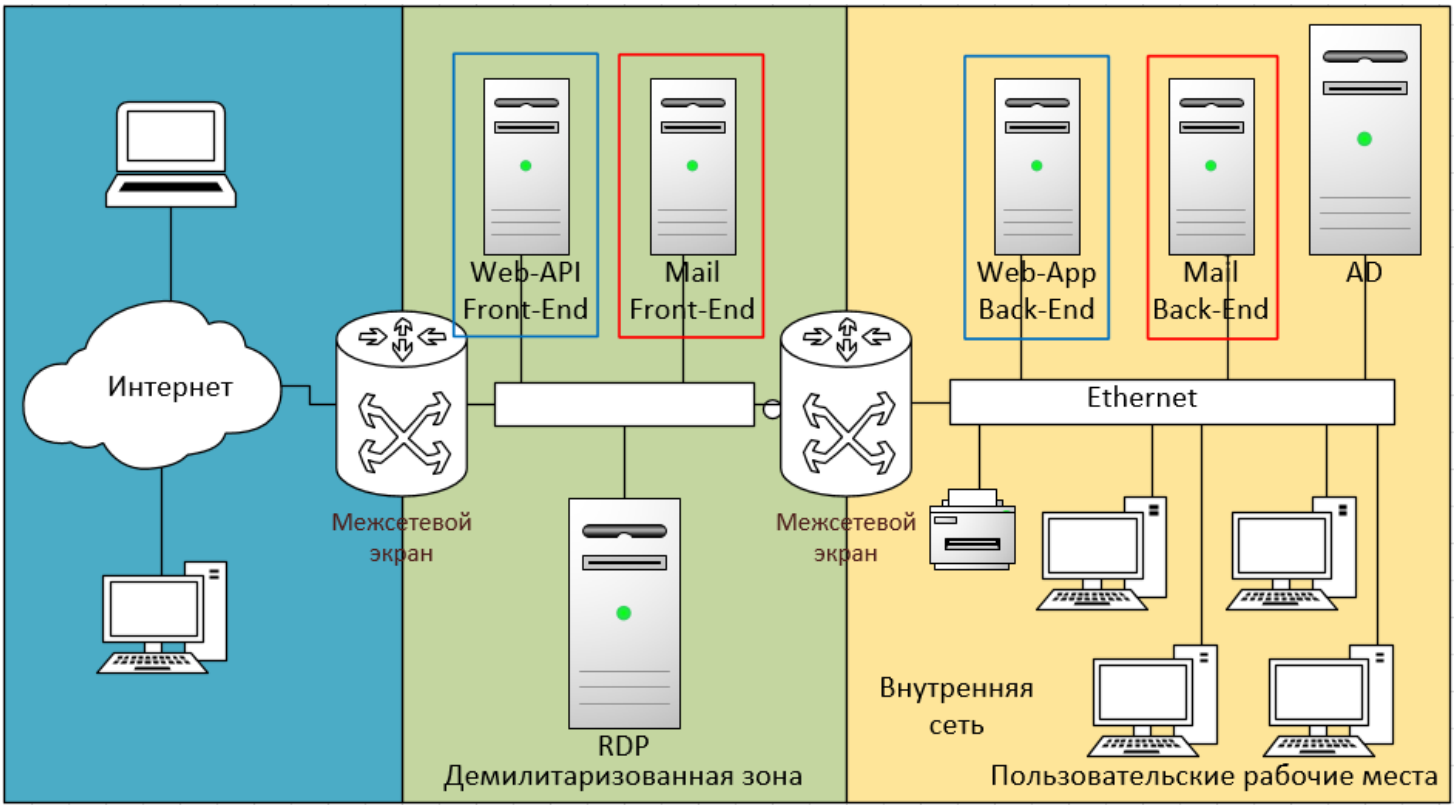

Рисунок 5. Схема удаленного доступа к локальной сети из интернета по варианту «Разделение сервисов на Front-End и Back-End»

Для взаимодействия Front-End и Back-End серверов одного сервиса необходимо настроить правила фильтрации пакетов на сетевых экранах, разрешающие взаимодействие серверов одного сервиса.

Плюсы варианта:

- Основным плюсом данного варианта является появление возможности защитить основную (рабочую) Back-End часть сервиса от атак, направленных на отказ сервиса в обслуживании. Это позволяет существенно снизить ущерб от таких атак, как TCP SYN Flood (атака, реализующая алгоритм отправки большого количества запросов на подключение по протоколу TCP в очень короткий период времени).

- Данный вариант предусматривает, что на Back-End сервере не будет доступа к сети Интернет. Это гарантирует, что в случае его взлома локально (например, локально запущенным вредоносным кодом) не будет возможности управлять сервером удаленно.
- Front-End сервер хорошо подходит для размещения на нем межсетевого экрана уровня приложений (например, Web application firewall) или системы предотвращения вторжений (IPS, например snort). [5]
- Если рассматривать защиту приложений, работающих через Web-интерфейс, то даже если сервер не поддерживает разнесение функций на Front-End и Back-End, применение http reverse proxy сервера (например, nginx) в качестве Front-End позволит минимизировать риски, связанные с атаками на отказ в обслуживании. Например, атаки типа TCP SYN flood могут сделать http reverse proxy недоступным, в то время как Back-End будет продолжать работать. [6]

Минусы варианта:

- Ограничение на инициацию соединений из демилитаризованной зоны во внутреннюю зону снижает функциональность используемого программного обеспечения. На практике серверам, находящимся в демилитаризованной зоне очень часто необходимо обращаться к серверам, находящимся во внутренней сети.
- Не все сервисы могут быть разделены на Front-End и Back-End части, но современные технологии разработки успешно нивелируют эту проблему.
- Реализация на межсетевых экранах правила, которое разрешает инициацию соединения из демилитаризованной зоны во внутреннюю сеть порождает угрозы, связанные с использованием данного правила со стороны других узлов.
- Политика информационной безопасности организации должна предусматривать мероприятия по защите серверов в демилитаризованной зоне.

Реализация защищенного доступа к локальной сети организации по варианту «Создание защищенного доступа в локальную сеть посредством реализации VPN с аутентификацией в Active Directory».

Данный вариант предусматривает реализацию виртуальной защищенной частной сети (VPN), которая классифицируется по архитектуре технического решения, как VPN с удаленным доступом.

Виртуальной защищенной сетью VPN (Virtual Private Network) называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную 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.
Сеть VPN позволяет с помощью туннелей VPN соединить центральный офис, офисы филиалов, офисы бизнес-партнеров и удаленных пользователей и безопасно передавать информацию через сеть Интернет (Рисунок 6).

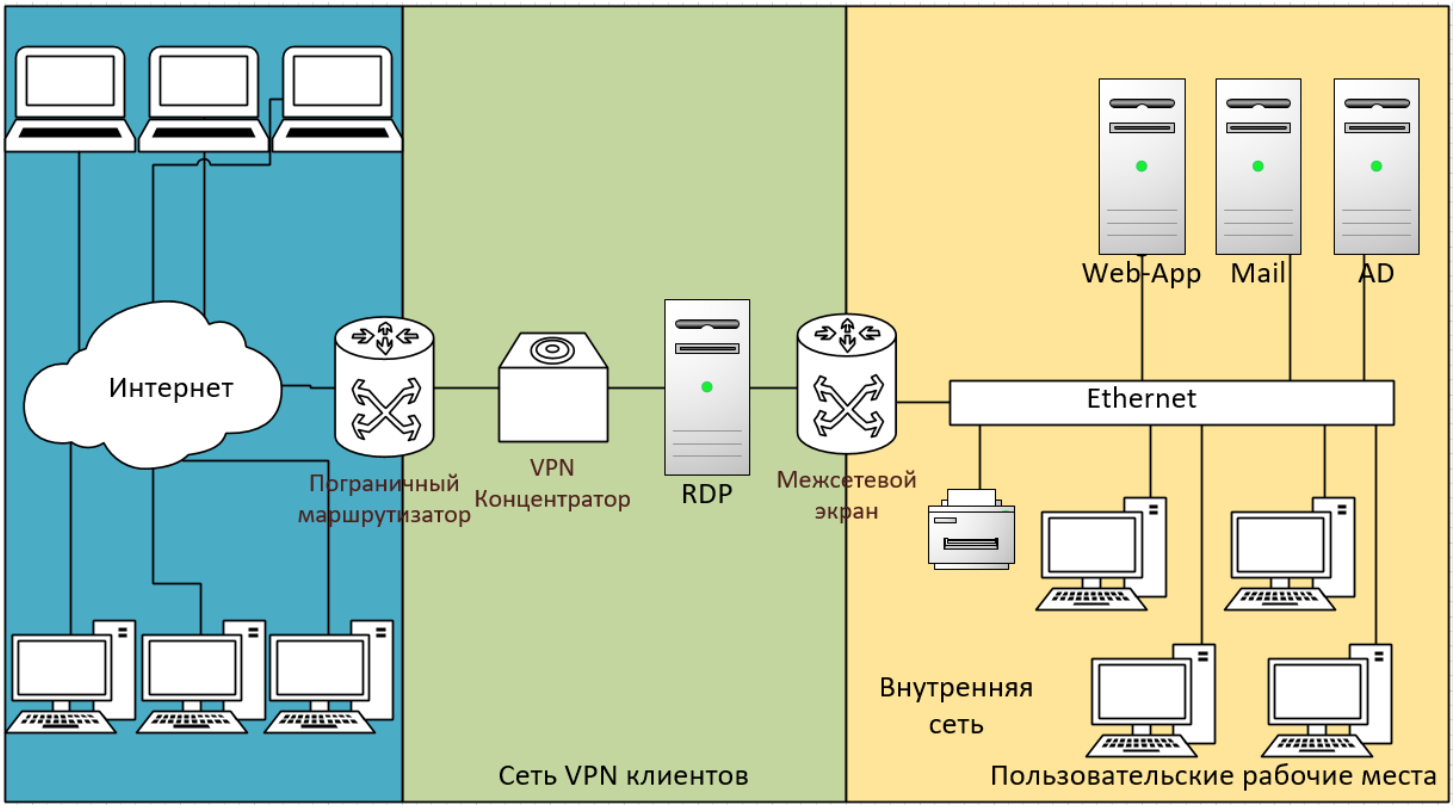

Рисунок 6. Схема удаленного доступа к локальной сети из интернета по варианту «Создание защищённого доступа в локальную сеть посредством VPN»

При реализации варианта доступа в локальную сеть посредством VPN предоставление доступа к ресурсам локальной сети происходит в соответствие со следующими этапами:

- Получение доступа через пограничный маршрутизатор поддерживающий протокол PPTP (туннельный протокол типа точка – точка) в изолированную сеть VPN-клиентов в составе которой находится VPN концентратор.

- Получение доступа по RDP к терминальному серверу.
- Получение непосредственного доступа к ресурсам локальной сети в соответствие с настроенными правами доступа.

Плюсы варианта:

- Данный вариант представляется наиболее безопасным именно для получения доступа к ресурсам локальной сети организации удаленными пользователями организации через сеть Интернет.
- Серверные части системы защищенного доступа можно организовывать на виртуальных машинах, организованных по технологиям Hyper-V или VMware.

Минусы варианта:

- Не удобен для реализации доступа к информационным сервисам компании всем пользователям.
- Требует дополнительного оборудования: Концентратор доступа по VPN.
- Требует высокой квалификации сетевых администраторов в организации.

Как видно из вышеперечисленных вариантов, существует множество технологий, позволяющих предоставить достаточно безопасный доступ пользователей (и сторонних сервисов) к ресурсам и сервисам локальных сетей организаций через сеть Интернет. Выбор технологии или компоновка решения из разных технологий зависит, прежде всего от состава ресурсов и сервисов, к которым необходим доступ, требований к безопасности и надежности от организации – владельца ресурсов и сервис.

Учитывая, что современные предприятия не могут быть конкурентоспособными на своих рынках без адекватной информационной поддержки, мобильных пользователей, без соответствующего информирования рынка, а также, принимая во внимание доступность оборудования и программного обеспечения для построения систем защищенного доступа к локальным сетям организации из сети Интернет, необходимо рассматривать гибридные система безопасного доступа. Такие системы позволяют обеспечить безопасный доступ и к ресурсам, и к сервисам локальной сети организации. Такие системы включают в себя следующие технологии (из вышеперечисленных):

- Создание демилитаризованной зоны.
- Разделение сервисов на Front-End и Back-End.

- Использование VPN с аутентификацией в AD для удаленного подключения к ресурсам корпоративной локальной сети.

В данной работе далее будут рассматриваться гибридные система безопасного доступа.

Технические решения для построения системы защищенного доступа к локальным сетям организаций из сети Интернет посредством организации VPN

Построение защищенных сетей с использованием технологии VPN предполагает следующие решения:

- На компьютер пользователя, которому необходимо получить удаленный доступ в локальную сеть через Интернет устанавливается VPN-агент. VPN-агент работает с пакетами протокола IP (по модели OSI).
- VPN-клиент необходим для автоматического шифрования всех исходящих данных и дешифрования всех входящих данных. VPN-клиент выполняет контроль целостности пакетов данных с помощью электронно-цифровой подписи или криптографической контрольной суммы, рассчитанной при помощи ключа шифрования.

Перед отправкой IP-пакета VPN-агент действует следующим образом:

Из нескольких поддерживаемых им алгоритмов шифрования и ЭЦП по IP-адресу получателя выбирает нужный для защиты данного пакета, а также ключи. Если же в его настройках такого получателя нет, то информация не отправляется [7]:

- определяет и добавляет в пакет ЭЦП отправителя или имитоприставку;
- шифрует пакет (целиком, включая заголовок);
- проводит инкапсуляцию, т. е. формирует новый заголовок, где указывается адрес вовсе не получателя, а его VPN-агента. Эта полезная дополнительная функция позволяет представить обмен между двумя сетями как обмен всего-навсего между двумя компьютерами, на которых установлены VPN-агенты. Всякая полезная для темных целей злоумышленника информация, например, внутренние IP-адреса, ему уже недоступна.

При получении IP-пакета выполняются обратные действия [8]:

- заголовок содержит сведения о VPN-агенте отправителя. Если таковой не входит в список разрешенных в настройках, то информация просто отбрасывается. То же самое происходит при приеме пакета с намеренно или

случайно поврежденным заголовком;
- согласно настройкам, выбираются алгоритмы шифрования и ЭЦП, а также необходимые криптографические ключи;
- пакет расшифровывается, затем проверяется его целостность. Если ЭЦП неверна, то он выбрасывается;
- пакет в его исходном виде отправляется настоящему адресату по внутренней сети.

Все операции выполняются автоматически. Сложной в технологии VPN является только настройка VPN-агентов, которая, впрочем, вполне по силам опытному пользователю [7]. VPN-агент может находиться непосредственно на защищаемом ПК, что полезно для мобильных пользователей, подключающихся к Интернет. В этом случае он обезопасит обмен данными только того компьютера, на котором установлен. Возможно совмещение VPN-агента с маршрутизатором (в этом случае его называют криптографическим) IP-пакетов. Ведущие мировые производители в последнее время выпускают маршрутизаторы со встроенной поддержкой VPN, например, Express VPN от Intel, который шифрует все проходящие пакеты по алгоритму Triple DES [8]. Как видно из описания, VPN-агенты создают каналы между защищаемыми сетями, которые называют “туннелями”. И действительно, они “прорыты” через Интернет от одной сети к другой; циркулирующая внутри информация спрятана от чужих глаз.

Кроме того, все пакеты “фильтруются” в соответствии с настройками. Таким образом, все действия VPN-агентов можно свести к двум механизмам: созданию туннелей и фильтрации проходящих пакетов.

Совокупность правил создания туннелей, которая называется “политикой безопасности”, записывается в настройках VPN-агентов. IP-пакеты направляются в тот или иной туннель или отбрасываются после того, как будут проверены [9]:

- IP-адрес источника (для исходящего пакета - адрес конкретного компьютера защищаемой сети);
- IP-адрес назначения;
- протокол более высокого уровня, которому принадлежит данный пакет (например, TCP или UDP);
- номер порта, с которого или на который отправлена информация (например, 1080).

По своей сути VPN обладает многими свойствами выделенной линии, однако развертывается она в пределах общедоступной сети, в данной работе рассматривается сеть Интернет. С помощью технологии туннелирования пакеты данных транслируются через общедоступную сеть как по обычному двухточечному соединению. Между каждой парой «отправитель–получатель данных» устанавливается своеобразный туннель – безопасное логическое соединение, позволяющее инкапсулировать данные одного протокола в пакеты другого [8]. Очень важным свойством туннелей является возможность дифференциации различных типов трафика и назначения им необходимых приоритетов обслуживания.

На Российском рынке существуют отечественные и импортные решения, позволяющие реализовать гибридные системы защищенного доступа к локальным сетям организации. Выбор конкретного решения зависит от требований к организации защищенного доступа.

Этапы проектирования систем защищенного доступа к локальным сетям организаций из сети Интернет

При проектировании системы защищенного доступа к локальной сети следует придерживаться определенной очередности этапов описания предметной области и проектирования системы (Таблица 1):

Таблица 1

Этапы проектирования системы защищенного доступа к локальной сети организации

№	Этап	Краткое описание
1	Описание текущего состояния системы доступа пользователей к ресурсам локальной сети	На данном этапе формируется описание текущей системы защищенного доступа с указанием имеющейся аппаратной базы и программного обеспечения

2	Формализация и классификация сервисов и ресурсов локальной сети организации	На этом этапе происходит определение перечня информационных ресурсов и сервисов которые будут опубликованы для доступа из сети Интернет
3	Категорирование пользователей ресурсов и сервисов локальной сети	Данный этап позволят определить категории пользователей, которым будут предоставляться доступы к ресурсам и сервисам
4	Определение требований по безопасности доступа по каждому ресурсу и сервису	На данном этапе формируется перечень требований, которым должна соответствовать система защищенного доступа к локальной сети
5	Выбор технологий для реализации системы защищенного доступа к локальной сети	На данном этапе происходит выбор технологий реализации системы защищенного доступа. Исходной информацией для выбора технологий являются данные, полученные на предыдущих этапах
6	Разработка технической архитектуры системы защищенного доступа	На этом этапе происходит выбор программно-аппаратного комплекса, который ляжет в основу системы защищенного доступа

Глава 2. Практическая часть

Разработка общей структуры

Локальная сеть организации «МИРАН» характеризуется следующими параметрами:

- Топология сети – звезда;
- Сеть построена по технологии Ethernet;
- Пропускная способность сети 100 Mb/s;

- Локальная сеть построена по технологии СКС. В качестве узловых коммутаторов используются Cisco WS-C2960+24PC-L (6 единиц);
- Количество персональных компьютеров в сети – 50 рабочих мест;
- В локальной сети установлено три сетевых принтера;
- Сеть организована по доменной технологии на основе контроллера домена службы Active Directory;
- В сети установлены следующие сервера:
    - Контроллер домена
    - Сервер приложений 1С
    - Сервер баз данных SQL с системой хранения данных
    - Почтовый сервер на базе Microsoft Exchange
    - Файловый сервер с подсистемой резервного копирования
    - Терминальный сервер для работы пользователей с программами 1С
    - Виртуальные сервера, реализованные на технологии Hyper-V, для реализации системы мониторинга ИТ инфраструктуры, системы Service Desk, корпоративного портала, сервера печати. Отдельный сервер выделен для работы корпоративной социальной сети Bitrix24.

Информационные ресурсы локальной

- Файловый сервер с установленными доступами по пользовательским ролям
- Сетевые принтера
- Корпоративное ПО 1С ERP

Информационные сервисы локальной сети

- Web интерфейс почтовой системы
- Система Service Desk
- Система Bitrix24

Внедрение программного и аппаратного обеспечения

У организации «МИРАН» в планах развития указано мероприятия по повышению мобильности сотрудников с целью оптимизации затрат на организацию рабочих мест пользователей. Принято решение часть пользователей перевести на удаленную работу из дома. В связи с этим возникла необходимость в реализации системы защищенного доступа к ресурсам и сервисам локальной сети организации.

Для создания удалённых рабочих мест пользователей в компании было проведен проект по внедрению системы Bitrix24 с целью интеграции всех сетевых ресурсов в единой рабочее информационное пространство. Использование Bitrix24 предполагает возможность удаленной работы пользователей с доступом через интернет в локальную сеть компании, для этих целей в организации сформировали следующие требования к системе защищенного удаленного доступа:

- Требования к безопасности:
  - Конфиденциальность. При подключении пользователей удаленно, система должна предоставлять возможность конфиденциального обмена информацией, вся информация, циркулирующая между пользователем и организацией, должна быть зашифрована;
  - Целостность сообщения. Система должна гарантировать, что информация, циркулирующая между пользователем и организацией, не будет изменена (случайно или злонамеренно).
  - Операционная безопасность. Система защищенного доступа должна иметь механизмы, противодействующие различным видам атак на работоспособность системы, на доступ к данным и т.д.
  - Система должна соответствовать современным требования в области информационной безопасности.
- Требования к надежности:
  - Система защищенного удаленного доступа должна иметь возможность функционирования в режиме 24x7;
  - Коэффициент доступности системы должен быть не менее 99,8;
- Требования к аппаратной платформе системы:
  - В компании предусмотрен отдел сопровождения ИТ инфраструктуры. Сетевые администраторы отдела имеют определенные компетенции по работе с оборудованием Cisco;
  - Форм-фактор оборудования должен обеспечивать размещение оборудования в стойке.

Контрольный пример реализации

В соответствии с этапами проектирования системы защищенного доступа, указанными в Таблице 1 сформируем проект системы.

- Описание текущего состояния системы доступа пользователей к ресурсам локальной сети.

На момент проектирования в организации «МИРАН» не предусмотрена система защищенного доступа к локальной сети и сети Интернет.

- Формализация и классификация сервисов и ресурсов локальной сети организации.

Для удаленного доступа разрешены следующие ресурсы:

-
  - Личные папки пользователей локальной сети;
  - Печать документов на сетевых принтерах организации;
  - Корпоративная информационная система 1С ERP;

Для удаленного доступа разрешены следующие сервисы:

-
  - Web интерфейс почтовой системы
  - Web интерфейс системы Service Desk
  - Web интерфейс системы Bitrix24
  - Десктопное и мобильное приложение системы Bitrix24
- Категорирование пользователей ресурсов и сервисов локальной сети

Пользователи организации классифицируются по ролям:

-
  - Менеджмент
  - Коммерсанты
  - Бухгалтерия
  - ИТ
  - Все пользователи
- Определение требований по безопасности доступа по каждому ресурсу и сервису
  - Доступ пользователей к файлам в их личных папках и к файлам в общих папках, хранящихся в дисковых массивах в системе хранения данных, определяется в соответствии с политикой прав доступа, настроенной в AD;
  - Доступ пользователей к принтерам определяется в соответствии с настроенными правами в AD;
  - Доступ пользователей к системе 1С ERP определяется в соответствии с настроенными правами в AD;
  - Сервисы почты и Service Desk интегрированы с AD, соответственно доступы к сервисам указаны в AD;

    - Доступы к системе Bitrix24 определяется в соответствующих административных настройках этой системы.
- Выбор технологий для реализации системы защищенного доступа к локальной сети

Исходя из требований организации и целей создания системы оптимальным решением будет использование технологии VPN для организации удаленного доступа к локальной сети организации с целью получения доступа к необходимым ресурсам и сервисам. При этом будут соблюдены следующие условия:

- Все средства обеспечения VPN будут размещены внутри предприятия;
- Организация самостоятельно защищает свои данные, размещая VPN-шлюзы и VPN-агенты в своей сети, на своей территории;
- В качестве аппаратной платформы в системе будет использовано оборудования Cisco;
- Технология создания VPN туннелей предполагает использования механизма Secured VPN – с защитой трафика;
- Для подключения удаленных работников будет использована технология Remote Access VPN с установкой на устройство работника VPN-агента;
- Учитывая требования по доступу к web ресурсам технология Clientless позволит подключаться к ресурсам через браузер;
- Для обеспечения требований по защите данных будет использована следующая конфигурация протоколов шифрования:
    - На канальном уровне: Протокол PPTP, который предусматривает как аутентификацию удаленного пользователя, так и зашифрованную передачу данных.
    - На сетевом уровне: Протокол IPSec предусматривает стандартные методы аутентификации пользователей или компьютеров при инициации туннеля, стандартные способы шифрования конечными точками туннеля, формирования и проверки цифровой подписи, а также стандартные методы обмена и управления криптографическими ключами между конечными точками.
    - На сеансовом уровне: Протокол SSL/TLS (Secure Sockets Layer/ Transport Layer Security), который создает защищенный туннель между конечными точками виртуальной сети, обеспечивая взаимную аутентификацию абонентов, а также конфиденциальность, подлинность и целостность циркулирующих по туннелю данных.
- Разработка технической архитектуры системы защищенного доступа

На Рисунке 7 указана основная технологическая архитектура решения системы защищенного доступа к локальной сети. На Рисунке 8 отражена программная архитектура системы.

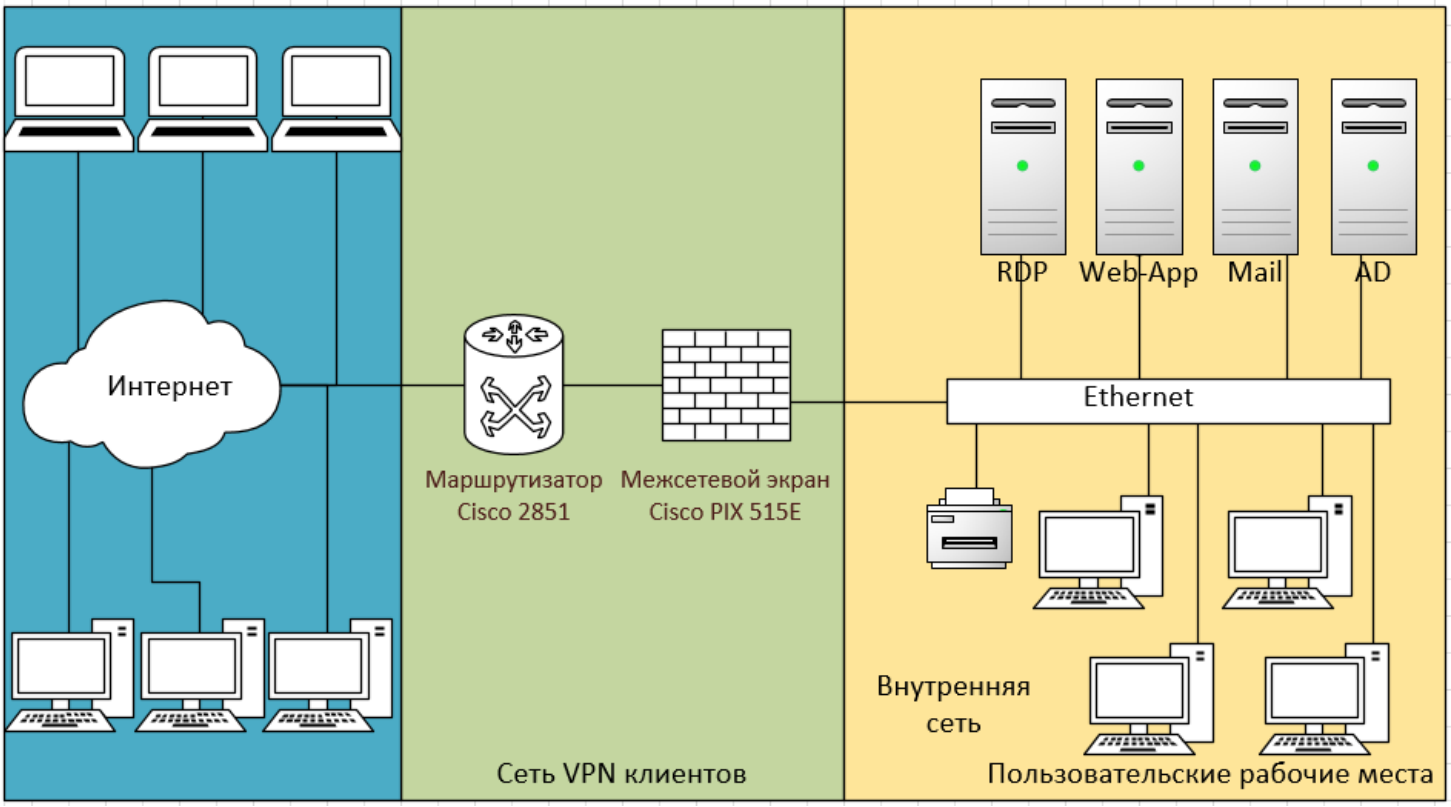

Рисунок 7. Схема удаленного доступа к локальной сети с использованием технологии «VPN»

В качестве ядра аппаратного обеспечения предлагается использоваться оборудование Cisco:

- Маршрутизатор с интеграцией сервисов Cisco 2851
- Межсетевой экран Cisco PIX Firewall 515E

Основные характеристики комплекта оборудования:

- 168-битовое шифрование 3DES IPsec VPN - 63 Мбит/с
- Одновременная поддержка 2000 VPN-туннелей
- Строгая система защиты от несанкционированного доступа на уровне соединения обеспечивает безопасность ресурсов внутренней сети
- Прозрачная поддержка всех основных сетевых услуг, таких как World Wide Web (WWW), File Transfer Protocol (FTP), Telnet, Archie, Gopher.

- Поддержка взаимодействий Microsoft Networking сервер — клиент, Oracle SQL Net сервер — клиент.
- Полный доступ к ресурсам сети Интернет для зарегистрированных пользователей внутренней сети.
- Поддержка интерфейсов Ethernet, Fast Ethernet, Token Ring и FDDI.
- Поддержка виртуальных частных сетей (Virtual Private Network) с использованием стандартной технологии IPSec.

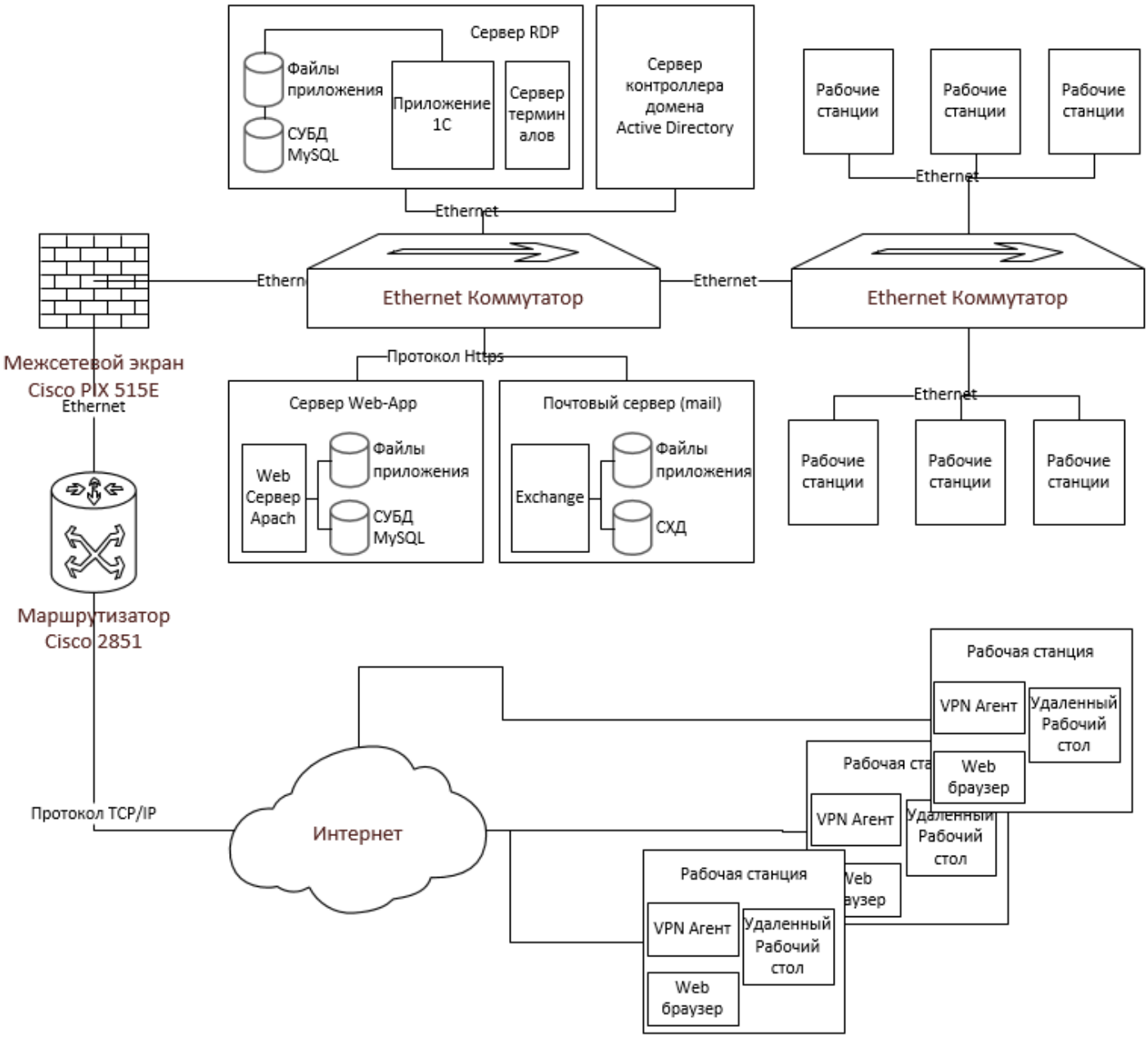

Рисунок 8. Программная архитектура системы защищенного доступа к локальной сети

В качестве примера на Рисунке 9 указана схема подмены IP-адресов при работе межсетевого экрана Cisco PIX 515 E

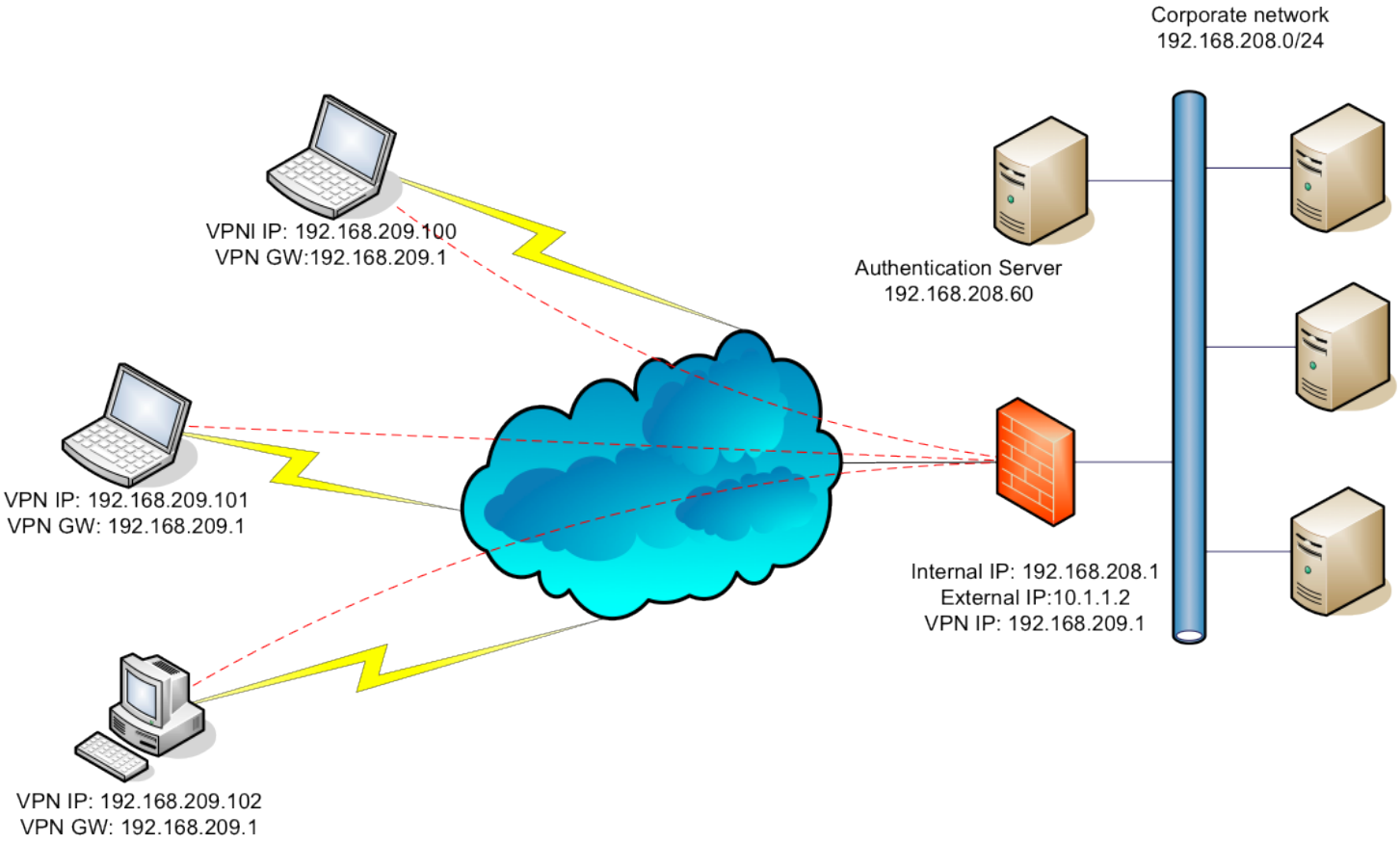

Рисунок 9. Схема подмены IP-адресов при работе межсетевого экрана

Выбранные технологии и набор оборудования полностью удовлетворяют требованиям организации «МИРАН» по проектированию системы защищенного доступа через Интернет к локальной сети компании. Подобранное оборудование, помимо невысокой стоимости, имеет развитые средства интерфейсной настройки, которые может освоить специалист, не обладающий высокими компетенциями сетевого инженера Cisco.

Заключение

В данной работе проведен анализ современных технологий реализации систем защищенного доступа к корпоративным локальным сетям. Акцент в анализе технологий сделан на подключения к локальным сетям удаленных корпоративных пользователей посредством глобальной сети Интернет. Стоит отметить, что

компании в своем развитии проходят стадии масштабирования, когда созданные филиалы компании располагаются территориально удаленного друг от друга. В этих случаях описанные технологии связи локальных сетей филиалов одной компании так же являются эффективными.

Наиболее сбалансированной по стоимости реализации и обеспечению информационной безопасности является технология создания частных защищенных виртуальных сетей. Данная технология позволяет шифровать передаваемые данные, что делает ее наиболее защищенной при использовании в компаниях любого размера. Технология VPN способна защитить передаваемые данные любого формата: текст, голос, видео и т.д.

В работе сделан акцент на то, что на самом деле является целью защищенного доступа – это ресурсы и сервисы локальной сети организации.

Результатом курсовой работы является подбор и проектирование системы и ее компонентов для создания защищенной среды доступа к локальной сети компании «МИРАН», при выполнении работы были определены этапы, которые необходимо выполнить для понимания объекта проектирования, требований к проектируемой системе, требований к безопасности проектируемой системы.

Список использованной литературы

1. Федеральный закон от 20 февраля 1995 г. N 24-ФЗ "Об информации, информатизации и защите информации"
2. Галатенко В.А. Идентификация и аутентификация, управление доступом. Лекция.
3. Джеймс Куроуз, Кит Росс «Компьютерные сети Нисходящий подход». – Москва, Издательство «Э», 2016. – 912 с.
4. Прокопенко А.Н. О содержании понятия информационные ресурсы в праве. Статья ВАК. Бизнес в законе. Экономико-юридический журнал, 2010 год.
5. Хаулет, Т. Инструменты безопасности с открытым исходным кодом / Т. Хаулет. - 2-е изд., испр. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 566 с. : ил.
6. Лапонина, О.Р. Протоколы безопасного сетевого взаимодействия / О.Р. Лапонина. - 2-е изд., исправ. - М. : Национальный Открытый Университет «ИНТУИТ», 2016. - 462 с.

7. Норманн Р. Выбираем протокол VPN /Windows IT Pro. – М.: Фаргус, 2005, − 15-26 с.
8. Петренко С. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных. – М.: Мир Internet, 2008, − 186-193 с.
9. Салливан К. Прогресс технологии VPN. PCWEEK/RE, – М.: Грей, 2009, − 128 с.
10. Домарев В.В. Безопасность информационных технологий. Системный подход: − К.: ТИД и ДС, 2004. − 312 с.
11. Завгородний В.И. Комплексная защита информации в компьютерных системах. − М.: Бука, 2009. – 524 с.
12. Корнеев И.К., Степанов Е.А. Информационная безопасность и защита информации. − М.: ИНФОРА−М, 2008. − 299 с.
13. Б. С. Гольдштейн, В. С. Елагин, Ю. Л. Сенченко. Телекоммуникационные протоколы. – СПб.: БХВ, 2011. – 138-149 с.
14. Малюк А.А., Пазизин С.В. Введение в защиту информации в авто-матизированных системах. − М.: Дрофа, 2010. – 52-61 с.
15. Попов Л.И., Зубарев А.В. Основные принципы повышения эффек-тивности реализации мероприятий по комплексной защите информации. – СПб.: Альтпресс, 2009. – 512 с.
16. Галямов В.А. Исследование и разработка моделей и методов оптимизации структур телекоммуникационных систем – Новосибирск.: − Новосибирский ГТУ, 2006. – 356-359 с.
17. Таненбаум Э.А. Компьютерные сети. − М.: ПИТ, 2010. – 34 с.
18. Семененко В.А. Информационная безопасность. М.: Брик, 2006. – 53 с.
19. Столяров Н.В. Понятие, сущность, цели и значение защиты информации. – М.: Конфидент, 2009. – 23 с.
20. Ярочкин В.И. Система безопасности фирмы. −М.: Брей, 2007. – 18 с.
21. Локальные сети – URL:http://www.stavtechno.stroyvitrina.ru/lokalnye-seti-37890.html.