МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»
Институт Систем Управления и Информационных Технологии
Кафедра «Системы информационной безопасности»

«ДОПУЩЕН К ЗАЩИТЕ»
Зав.кафедрой _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: «Разработка защищённой сети интранет на основе инструментальных средств создания VPN.»

Специальность Системы Информационной Безопасности_____

Выполнил(а) Бекетаева Гаухар Айдарқызы_____ Группа СИБ-16-2_____
(Ф.И.О.)

Научный руководитель к.т.н., доцент Шайкулова Актоты Алиевна_____
(ученая степень, звание, Ф.И.О.)
Консультанты: старший преподаватель Альмуратова Камшат Бимуратовна
по специальной части:
старший преподаватель Дмитриева Маргарита Валерьевна _____

_____ «_____» _____20____г.
(подпись)

по безопасности жизнедеятельности:
к.т.н. доцент Приходько Николай Георгиевич_____

_____ «_____» _____20____г.
(подпись)

Нормоконтролер: старший преподаватель Дмитриева Маргарита Валерьевна_
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Рецензент: _____
(ученая степень, звание, Ф.И.О.)
_____ «_____» _____20____г.
(подпись)

Алматы 2020

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ ИМЕНИ ГУМАРБЕКА ДАУКЕЕВА»

Институт Систем Управления и Информационных
Кафедра «Системы Информационной Безопасности»
Специальность «Системы Информационной Безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Бекетаевой Гаухар Айдаркызы
(Ф.И.О.)

Тема проекта «Разработка защищённой сети интранет на основе инструментальных средств создания VPN»

Утверждена приказом по университету № 147 от «11» ноября 2020 г.

Срок сдачи законченного проекта «_1___» ____июня_____ 2020 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): _____

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: Цель работы – Спроектировать защиту каналов передачи данных между ЦО Банка, его филиалами, УДО и устройствами самообслуживания, агентской сетью, разработчиков.

Перечень графического материала (с точным указанием обязательных чертежей): схема виртуального маршрута и сети, расположение и методы подключения необходимых компонентов и информационной системе.

Основная рекомендуемая литература: Магический квадрант для управления информацией о безопасности и событиями Оливер Рочфорд, Келли Кавана. Книга Управление рисками безопасности: построение программы управления рисками информационной безопасности с нуля Эван Уиллер.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Анализ рисков информационной безопасности	старший преподаватель Дмитриева Маргарита Валерьевна	17.02.2020 – 09.05.2020	

Безопасность жизнедеятельности	к.т.н. доцент Приходько Николай Георгиевич	17.02.2020 – 09.05.2020	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Проектирование сети банка	17.02.2020 – 20.02.2020	
Открытие сетевых доступов. Предоставление привилегий и ролей	21.02.2020 – 28.02.2020	
Организация системы тунелирования VPN	01.03.2020 – 08.03.2020	
Настройка сетевых интерфейсов на маршрутизаторе	09.03.2020 - 18.03.2020	
Организация различных видов аудита	19.03.2020 – 27.03.2020	
Организация защиты сети. Сетевое шифрование. Создание схем коммутации на основе протокола MPLS VPN.	28.03.2020 - 07.04.2020	
Администрирование системы по предоставлению удаленного доступа	08.04.2020 - 30.04.2020	
Анализ рисков ИБ. БЖД	01.05.2020 - 09.05.2020	

Дата выдачи задания «_____»_____20___г.

Заведующий кафедрой _____ (_____)
(подпись) (ФИО)

Научный руководитель проекта _____ (_____)
(подпись) (ФИО)

Задание принял к исполнению студент _____ (_____)
(подпись) (ФИО)

Аңдатпа

Дипломдық жобада ФПСУ-IP бағдарламалық кешені негізінде банктің қорғалған желісі әзірленді, MPLS протоколы негізінде VPN желісі жобаланды, MPLS-ді қосу және пакеттерді белгілер бойынша тарату үшін маршрутизаторда интерфейстерді баптау жүргізілді.

Өміртіршілік қауіпсіздігі бойынша тарау қолайлы еңбек жағдайларын сипаттайды. Тәуекелдерді талдау және бағалау тарауында қауіптердің туындау ықтималдығын азайту жөніндегі шараларды қолданғанға дейін және одан кейін тәуекелдер деңгейінің екі параметрлері бойынша есептер келтірілген.

Аннотация

В дипломном проекте разработана защищенная сеть Банка на основе программного комплекса ФПСУ-IP, спроектированы сети VPN на основе протокола MPLS, проведены настройки интерфейсов на маршрутизаторе для подключения MPLS и передачи пакетов по меткам.

Глава по безопасности жизнедеятельности характеризует благоприятные условия труда. В главе анализ и оценка рисков были приведены расчеты по двум параметрам уровня рисков до и после применения мер по уменьшению вероятности возникновения угроз.

Annotation

In the diploma project, a secure Bank network was developed based on the FPSU-IP software package, VPN networks were designed based on the MPLS Protocol, and interfaces were configured on the router for connecting MPLS and transmitting packets by tags.

The Chapter on life safety describes favorable working conditions. In the Chapter risk analysis and assessment, calculations were made for two parameters of the risk level before and after the application of measures to reduce the likelihood of threats.

Содержание

Введение

В последнее время в мире телекоммуникаций наблюдается повышенный интерес к виртуальным частным сетям (VPN). Это связано с необходимостью снижения затрат на обслуживание корпоративной сети за счет более дешевого соединения между удаленными офисами и удаленными пользователями через Интернет. На самом деле, когда вы проводите сравнение затрат на подключение сервиса к большему количеству сетей в сети, например, к сети Frame Relay, то можно заметить существенную разницу в цене. Однако важно отметить, что при объединении сетей Интернета сразу же всплывает вопрос о сохранности данных, поэтому необходимо создавать механизмы обеспечения конфиденциальности и целостности передаваемой информации. Сети, на основе такого механизма именуемые виртуальной частной сетью.

Кроме того, очень часто современному человеку, занимающемуся развитием собственного бизнеса, приходится много путешествовать. Это может быть путешествие в отдаленные уголки страны или в чужие страны. Это не редкость для людей, которые имеют доступ к своей информации, хранящейся на их домашнем компьютере или компьютере компании. Эту проблему можно решить, запустив удаленное соединение через модем и телефонную линию. Использование телефонной линии имеет свои особенности. Минусы такого решения заключаются в том, что звонок из другой страны стоит немалых денег. Нет никакого другого решения, которое называется VPN. Преимущества технологии VPN заключаются в том, что организация удаленного доступа осуществляется по телефонной линии, но через интернет, это очень дешевле и лучше. На мой взгляд, технология VPN имеет широкий кругозор по всему миру.

1 Понятие и классификация VPN сетей, их построение

1.1 Что такое VPN

Виртуальная частная сеть (Virtual Private Network) - это логическая сеть, построенная на другой сети, например в Интернете. Несмотря на то, что связь должна осуществляться по сети с использованием незащищенного протокола шифрования, создается канал для обмена персональной информацией третьей стороной. VPN позволяет объединить несколько отделов внутри организации и в сети с помощью непроверенных каналов для связи друг с другом.

В рамках VPN существует много информации по одной выделенной линии, она распределяется внутри сети. При использовании метода туннелирования пакет данных передается по общедоступной сети, например, по обычному двухточечному соединению. По умолчанию защищенный туннелем логический тип связи устанавливается между каждой парой передачи / приема данных, что позволяет инкапсулировать данные в пакет протокола в сеть. Основными компонентами туннеля являются:

- инициатор;
- маршрутизируемая сеть;
- туннельный коммутатор;
- один или несколько туннельных терминаторов.

Сам по себе принцип работы VPN не противоречит базовым сетевым технологиям и протоколам. Когда соединение удаленного доступа установлено, клиент отправляет поток пакетов в протоколе PPP, как сервер. В случае виртуальных выделенных линий между локальными сетями их маршрутизаторы также обмениваются пакетами PPP. Однако принципиально новый пункт-Загрузка пакета через защищенный туннель, организованный в рамках публичной сети.

Выходной код позволяет организовать передачу пакета по протоколу в логической среде, используемой для другого протокола. В результате появляется возможность решать задачи интероперабельности в различных сетях, возникает необходимость обеспечения целостности и конфиденциальности передаваемых данных, для того чтобы преодолеть несоответствия внешнего протокола или схемы маршрутизации.

Существующая сетевая инфраструктура компании может быть подготовлена на основе использования виртуальных частных сетей, вплоть до программно-аппаратных средств. Организацию виртуальной частной сети можно сравнить с передачей данных по глобальной сети. Как правило, прямое соединение между удаленным пользователем и конечной точкой туннеля устанавливается по протоколу PPP.

Наиболее распространенным методом создания VPN-туннелей является инкапсуляция сетевых протоколов (IP, IPX, AppleTalk и т. д.). в PPP, а затем инкапсулировать пакеты, которые формируются в протокол туннелирования. Обычно это интернет, или (реже) банкомат и Frame Relay. Этот подход был

назван туннелированием второго уровня, потому что пассажир " это второй уровень протокола.

Альтернативный подход заключается в инкапсуляции пакетов сетевого протокола непосредственно в туннельный протокол (например, VTP), который называется третьим уровнем кода выхода.

1.2 Классификация VPN сетей

Можно классифицировать VPN решения по нескольким основным параметрам:

1. В зависимости от типа используемой среды:

а) защищенная сеть VPN. Самая распространенная версия частной сети. Вы можете создать надежную и безопасную их работу на базе ненадежной сети, как правило, интернета. Примерами безопасных VPN являются: IPSec, OpenVPN и PPTP.

б) доверенная сеть VPN. Он используется в тех случаях, когда передача в окружающую среду может считаться надежной и вам просто нужно быть на задаче создания виртуальной подсети внутри более крупной сети. Вопросы безопасности стали неуместными. Примеры такого VPN-решения: у кабельных компаний нет и L2TP. Точнее будет сказать, что это руководящие принципы для передачи одной безопасности или присвоения другой, например, L2TP обычно используется в сочетании с IPSec.

2. По способу его осуществления:

а) сеть VPN представлена в виде специального программного и аппаратного обеспечения. Реализация VPN-сети осуществляется с помощью специального набора программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, в целом, высокий уровень безопасности.

б) сеть VPN представлена в виде программного решения. Использование персонального компьютера со специальным программным обеспечением, обеспечивающим функциональность VPN.

в) сеть VPN с интегрированным решением. Функциональность VPN обеспечивает комплексное принятие решений, а также решение задач фильтрации сетевого трафика, организации брандмауэра и качества обслуживания.

3. По назначению:

а) Intranet VPN. Он используется во многих распределенных филиалах одной и той же организации, которые могут быть сгруппированы в защищенную сетевую связь через открытые каналы связи.

б) Remote Access VPN. Он используется для создания защищенного канала между сегментом корпоративной сети (центральный офис или дочерняя компания) и индивидуальным пользователем, работающим из дома, заключается в подключении корпоративных ресурсов с домашнего компьютера или в командировке, а также для подключения корпоративных ресурсов через ноутбук.

в) Extranet VPN. Использование сети, к которой подключены "внешние" пользователи (напр. пользователи или клиенты) подключаются. Уровень доверия к ним значительно ниже, чем к компании самого сотрудника, и поэтому необходимо предусмотреть специальные защитные "пороги", которые препятствуют или ограничивают доступ к последней, особенно важной и конфиденциальной информации.

4. По типу протокола:

Существует реализация VPN под TCP / IP, IPX и AppleTalk. Однако сегодня наблюдается тенденция к универсальному переходу на протокол TCP/IP, а также абсолютное большинство VPN-решений и поддержка его.

5.По уровню сетевого протокола:

На основе сопоставления уровня сетевого протокола в эталонной сетевой модели ISO / OSI.

Виртуальные частные сети реализуются с использованием протоколов туннелирования данных через общедоступную сеть Интернет-связи, а также с использованием протоколов туннелирования, которые шифруют данные и передают их из конца в конец между пользователями. Как правило, для создания VPN-сети используются следующие уровни протокола: канальный уровень, сетевой уровень, транспортный уровень.

1.3 Протоколы VPN сетей

Так как данные виртуальной частной сети передаются через разветвленную сеть, так что они будут защищены от посторонних глаз. Для осуществления работы по передаче информации существует и множество методических рекомендаций, предназначенных для защиты VPN, но их следует разделить на два типа, и они работают совместно:

- протоколы, инкапсулирующие данные и формирующие VPN соединение;
- протоколы, шифрующие данные внутри созданного туннеля.

Первый тип-это протокол, определяющий Connection-соединение, а второй тип-ответ непосредственно на шифрование данных.

К первому типу протоколов относятся, например, протоколы PPTP и L2TP.

PPTP (Point-to-Point Tunneling Protocol)-протокол туннелирования, "точка-точка является расширением PPP (Point-to-Point Protocol), поскольку он использует механизмы аутентификации, сжатия и шифрования. Протокол PPTP встроен в клиент удаленного доступа Windows. По умолчанию для протокола вы должны использовать mppe-шифрование (Microsoft Point-to-Point Encryption). Также можно передавать данные без шифрования в открытом формате.

Инкапсуляция информации в протокол PPTP происходит в том случае, когда добавляется заголовок GRE туннель и IP-заголовок данных, обрабатываемых протоколом PPP.

Рисунок 1.1 - Структура PPTP-пакета

На рисунке 1 рамка PPTP имеет направляющую-пакет включает в себя следующие поля:

- IP-дейтаграмма - исходный пакет локальной сети, содержащий пользовательские данные и IP-заголовок локальной адресации;

- PPP-заголовок и - GRE-заголовок - данные, необходимые для создания и поддержания VPN-туннеля;

- IP-заголовок - реальный IP-адрес VPN-шлюза назначения и другие данные для передачи пакета через Интернет между входами туннеля.

PPP (англ. Point - to-Point Protocol) - протокол на сетевом уровне модели OSI, который используется в различных формах физических сетей, а также для создания каналов связи между двумя узлами, верификации программного обеспечения, шифрования и сжатия данных.

GRE (англ. Generic Routing Encapsulation) - протокол ченнелинга, выполнение пакета сетевого уровня в IP-сеть, пакетов в другую сеть.

L2TP (Layer Two Tunneling Protocol) - более совершенный сервис. Он обеспечивает более безопасное соединение вместо PPTP, шифрование осуществляется в рамках протоколов IPSec (IP security). L2TP также имеет встроенный клиент удаленного доступа Windows.

Инкапсуляция данных осуществляется путем добавления заголовков L2TP и IPSec к данным протокола уведомления PPP. IPSec (IP security Protocol) - это современный набор протоколов, обеспечивающих безопасность при установлении VPN-соединения, аутентификации, доступе и контроле. IPSec работает на сетевом уровне эталонной модели взаимодействия, и это позволяет создавать шифрование VPN-туннелей или кодировать трафик между двумя узлами. Тип сервиса IPSec, он включает в себя протоколы: AH (Autentation of the Object) - проверка подлинности источника и целостности сообщения, ESP (Encapsulating Security полезная нагрузка) шифрование сообщения.

PPTP используют порт назначения для создания сети для управления туннелем. Эта процедура выполняется на уровне передачи модели OSI. После того как вы создали туннель, клиент и сервер, вы можете начать с совместного использования служб пакета. Кроме того, PPTP-соединение с управлением, которое обеспечивает целостность канала, создает соединение для передачи данных через туннель данных. Инкапсуляция данных перед тем, как вы На канальном уровне передачи данных может использоваться один уровень,

протоколы передачи данных L2TP и PPTP, которые используют утверждение и аутентификацию.

В настоящее время наиболее распространенным протоколом VPN является протокол point-to-point channeling protocol, или протокол point-to-point channeling protocol-PPTP. Он был разработан 3Com и Microsoft для обеспечения безопасного удаленного доступа к корпоративным сетям через Интернет. PPTP использует а на текущем открытом стандарте TCP / IP и в значительной степени основан на старом PPP PPP, протоколе связи. На практике RRR остается с протоколом для связи между rrtr и совещанием. RRTR создает туннель через сеть к серверу NT получателю и отправляет удаленному пользователю пакет RRR для данного события. Сервер и рабочая станция используют виртуальную частную сеть, и не беспокойтесь о ней, поскольку она предоставлена или доступна всей сети, является одним из них. Сервер - run off, в отличие от специализированных серверов удаленного доступа, позволяющих использовать сеть устройств, администраторы не должны недооценивать это пользователи системы безопасности Windows NT server.

Несмотря на то, что пропускная способность протокола относится только к устройствам, работающим на Windows, он предоставляет компании возможность взаимодействовать с текущей сетевой инфраструктурой и наносит ущерб системам безопасности. Таким образом, удаленный пользователь может подключиться к интернету через локального поставщика услуг для аналоговой телефонной линии или канала ISDN настроить параметры подключения к серверу NT. Однако компании не приходится тратить большой объем на организацию и обслуживание пула, модемного соединения, которое обеспечивает удаленный доступ к сети.

Кроме того, необходимо учитывать функцию ППТР. PPTP конденсирует IP-пакет для передачи по IP-сети. Клиенты отправите их через туннель, вам нужно будет сделать это немного по-другому время от времени-это обычная кража со взломом. Инкапсуляция данных перед отправкой их в туннель включает в себя два этапа:

1 создается информационная часть PPP. Данные проходят от прикладного уровня OSI до канального;

2. затем данные передаются в модель OSI и инкапсулируются на верхнем и протокольном уровнях.

Таким образом, в ходе второй фазы данных достигается уровень передачи. Однако эта информация может быть размещена, а может и не быть размещена, как и следовало ожидать, потому что канал для уровня OSI, на котором она находится, несет за нее ответственность. Следовательно, PPTP шифрует поле полезной нагрузки пакета, и предполагается, что уровень, на котором он обычно принадлежит PPP, который должен быть добавлен в заголовок и PPTP-пакет для PPP до конца. В этот момент времени, в момент установления каркаса поверхность отделывается.

Кроме того, PPTP инкапсулирует кадр PPP внутри пакета в маршрутизацию конденсации (GRE), которая является частью сетевого уровня.

GRE конденсирует протоколы сетевого уровня, такие как IPX, AppleTalk, DECnet, и предоставляет им возможность передавать данные в IP-сеть. Однако GRE больше не может устанавливать рабочее время и защищать ваши данные от злоумышленников. Это использует PPTP возможность создавать соединение и взаимодействовать с ним. Использование инкапсуляции в качестве метода блокировки позволяет ограничить пропускную способность PPTP только в IP-сети.

После того, как фрейм PPP инкапсулируется в рамках правильной инкапсуляции, он инкапсулируется в рамках права ИС. Заголовок IP содержит адреса как отправителя, так и получателя пакета. В заключение PPTP добавляет заголовок PPP и конец.

Система передачи данных через туннель. Если ваша целевая система должна избавиться от всех заголовков службы, оставив только данные PPP.

В ближайшее время, а также в связи с увеличением числа дистрибутивов виртуальных частных сетей, нам придется ждать на Земле нового туннельного протокола, второго уровня, туннельного протокола уровня 2-к протоколу L2TP.

L2TP - это результат комбинации протоколов PPTP и L2F (переадресация уровня 2). PPTP позволяет отправлять пакеты PPP по туннелю, в то время как L2F включает пакеты SLIP и PPP. Чтобы избежать путаницы и проблем связи на телекоммуникационном рынке, Internet Engineering Task Force (IETF) предложила Cisco Systems, объединяющую PPTP и L2F. во всех расчетах протокол L2TP реализован в лучших вариантах PPTP и L2F. основное преимущество L2TP связано с тем, что сервис позволяет создавать туннели, к сожалению, реализация L2TP в Windows 2000 поддерживается только на IP.

Особенности PPTP и L2TP очень сильно отличаются. L2TP может использоваться только в IP-сети, провайдер, поставщик сообщений должен использоваться в том же формате и протоколе, который используется для генерации и приема данных через туннель. PPTP можно использовать в IP-сети и иметь отдельное TCP-соединение для создания, и вы можете использовать его. L2TP через IPSec обеспечивает несколько уровней безопасности, чем PPTP, а также может гарантировать почти 100% безопасность информации, которая имеет отношение к вашему бизнесу. Свойства L2TP делают протокол чрезвычайно перспективным для создания виртуальной сети.

Протоколы L2TP и PPTP отличаются от третьего уровня, протокола воронки, который используется для широкого спектра функций:

1. дайте компании возможность выбрать способ аутентификации пользователя, а также определить свою собственную юрисдикцию в "общественном месте " или у интернет-провайдера. При обработке PPP для перехода пакета на хосты в корпоративной сети для получения всей необходимой информации они должны быть в состоянии идентифицировать клиента.

2. преобразование туннеля, поддержка: в конце туннеля, и начинает его с любого другого из многих возможных Терминаторов. Поворот туннеля позволяет расширить PPP-соединение до нужной конечной точки.

3. они позволят вам подключаться к корпоративной сети, системным администраторам для реализации политики, назначать права доступа пользователям, например, непосредственно на стене, а также к внутреннему серверу. Чтобы они могли действовать как истребители ... туннели получают PPP-пакет с информацией для пользователя, они могут быть способны реализовать стратегии безопасности, сформулированные отдельными пользователями, менеджерами пропускной способности. (Код третьего уровня, выход не главное, из пакета, а стратегия безопасности, фильтр должен быть применен к поверхности канала, диапазон сетевых устройств. Кроме того, если вы используете туннельный коммутатор, вы можете организовать "продолжение" второго уровня туннеля и направить передачу трафика отдельных пользователей на их соответствующие внутренние серверы. Эти серверы могут быть нацелены на дальнейшую фильтрацию пакета.

Кроме того, уровень и фон уличной организации туннелей могут быть использованы для кабельных компаний не по технологии.

Из англ.-multiprotocol Label Switching-data data labels-устройство передачи данных, имитирующее различные информационные сети по каналам связи через сеть с включенными пакетами. Кабельные компании работают не на том уровне, где их можно разместить в одном, а на третьем сетевом уровне модели OSI, и поэтому обычно называют канально на уровне сетевого протокола. Он был разработан для того, чтобы обеспечить услугу передачи данных в клиентские сети по каналам и сети по пакету. С помощью кабельных компаний этого не делают, вы можете отправлять трафик в более разнообразную природу, такую как IP-пакет, ATM, SONET и Ethernet-фреймы.

Решения об организации VPN на уровне канального уровня передачи данных должны иметь довольно ограниченный диапазон, хотя, как правило, в контексте сферы услуг.

Сетевой уровень (уровень IP). Используется протокол IPSec, который реализует шифрование и Конфедерацию данных и аутентификацию подписчиков. Использование IPSec обеспечивает полный доступ, эквивалентный физическому подключению к корпоративной сети. Чтобы установить VPN, каждый участник должен настроить определенные параметры IPSec, таким образом каждый клиент должен иметь программное обеспечение, реализующее IPSec.

Конечно, ни одна компания не хотела бы открыто передавать в финансовая интернет или другая конфиденциальная информация. VPN-каналы защищены мощными алгоритмами шифрования, встроенными в стандарты протокола безопасности IPSec. IPSec или Internet Protocol Security-стандарт, выбранный международным сообществом, группа IETF-Internet Engineering Task Force, создает основы безопасности для интернет-протокола (IP / IPSec обеспечивает защиту на сетевом уровне и требует поддержки стандарта IPSec только общаются друг с другом устройства по обе стороны соединения. Все остальные устройства, расположенные между ними, просто обеспечивают трафик IP-пакетов.

Как люди, использующие технологию IPSec, взаимодействуют, как правило, определяется термином "защищенная ассоциация" - Ассоциация безопасности (SA). Защищенная ассоциация действует на основе соглашения, заключенного сторонами, которые используют средства IPSec для защиты информации, передаваемой друг другу. Это соглашение регулирует несколько параметров: IP-адреса отправителя и получателя, криптографический алгоритм, порядок обмена ключами, размер ключей, продолжительность ключей, алгоритм аутентификации.

IPSec -это последовательный набор открытых стандартов с ядром, который можно просто интегрировать с новыми функциями и протоколами. Ядро IPSec состоит из трех протоколов:

AH или Authentication Header-заголовок аутентификации-обеспечивает целостность и подлинность данных. Основная цель протокола AH позволяет принимающей стороне убедиться, что:

- пакет был отправлен стороной, с которой была установлена безопасная связь;
- содержимое пакета не было изменено во время передачи по сети;
- пакет не является дубликатом уже полученного пакета.

Первые две функции являются обязательными для протокола AH, а последняя выбирается при установлении привязки по желанию. Для выполнения этих функций протокол AH использует специальный заголовок. Его структура рассматривается по следующей схеме:

Поле Next header (next header) указывает код протокола верхнего уровня, то есть протокол, сообщение которого помещено в поле данных IP-пакета.

Поле длина полезной нагрузки (payload length) содержит длину заголовка AH.

Индекс параметров безопасности (SPI) используется для привязки пакета к предусмотренной хорошей привязке.

Поле order of a few (SN) указывает на порядок следования нескольких пакетов и используется для защиты его от ложного воспроизведения (если третья сторона пытается изначально перехватить защищенные пакеты, отправленные авторизованным отправителем).

Поле аутентификационных данных, содержащее так называемое значение проверки целостности (ICV), используется для проверки и сертификации целостности пакета. Это значение, также известное как дайджест, вычисленное с использованием одной из двух вычислительных функций, не должно быть изменено функцией, поддерживаемой протоколом MD5 или LEGITIMATE-1, но какие другие функции могут быть использованы.

SP или Повышение платы за безопасность-на основе данных из самых сложных-усложняют отправленные данные, обеспечивают конфиденциальность, могут также поддерживать аутентификацию и целостность данных;

Протокол ESP решает эти две группы задач.

Первый относится к деятельности, аналогичной для людей, использующих протокол AH, который обеспечивает аутентификацию и целостность данных на основе дайджеста,

Во-вторых, защита данных, отправленных усложнением, которого он не видел.

Головка разделена на две части, разделенные полем данных. Первая часть, называемая ESP head, состоит из двух полей (SPI и SN), одна и та же цель-AH protocol field с тем же именем и помещается перед полем данных.

Так же, как и другие поля протокола ESP, называемые ESP The pit stop, расположенные в конце пакета.

Два увольнения поля-следующего руководителя и утверждение данных-то же самое с AH руководителем поля. Ратификация данных terrain не существует, если вы решите не использовать протокол ESP integrity keupayaan, если сделаете хорошую привязку. В дополнение к этим полям, увольнение содержит два дополнительных поля места и держателей места, которые долго.

Протоколы AH и ESP могут защитить данные в двух модулях:

- в каретке-удаление производится исходящим IP-заголовком;

- в туннеле-происхождение пакета вставляется в новый IP-пакет и перемещение выполняется с помощью заголовка new.

Возможности протокола AH и ESP несколько перекрываются: протокол AH отвечает только за обеспечение целостности и аутентификацию данных, протокол ESP может усложнять данные и, кроме того, выполнять функции протокола AH (в виде франшизы). ESP может поддерживать функции шифрования и аутентификации / целостности в любых комбинациях, то есть либо всю группу функций, либо только аутентификации, либо только шифрование.

IKE или Internet Key Exchange-обмен интернет-ключами-решает вспомогательную задачу автоматического предоставления конечным точкам защищенного канала секретных ключей, необходимых для работы протоколов аутентификации и шифрования данных.

На транспортном уровне безопасность и защиту здоровья используются в работе/TLS или Secure Socket Layer/Transport Layer Security, которая реализует криптографию и подлинности передачи уровней получателя и передатчика. Безопасность и здоровье на работе / TLS может использоваться для защиты TCP движение, не может применяться для защиты трафика UDP. Для работы VPN-на основе безопасность и охрану здоровья на работе / TLS не требуется специальное программное обеспечение, так как каждый браузер и почтовый клиент оснащены эти протоколы. Потому что безопасность и здоровье на работе / TLS реализуется на транспортном уровне, установлено безопасное сквозное подключение.

TLS-протокол основан на протоколе SSL 3.0 и Netscape состоит из двух Частей: TLS Record Protocol TLS Handshake Protocol. Разница между безопасности и гигиены труда 3.0 и TLS 1.0 меньше.

Безопасность и здоровье на работе / TLS включает в себя три основных этапа: 1) диалог между сторонами для выбора криптографического алгоритма; 2) обмен ключами на основе шифрования шифрования системы или сертифицированный проверки подлинности 3) передача зашифрованных данных с использованием симметричных алгоритмов шифрования.

1.4 Создание VPN

Существуют различные варианты для создания VPN. При выборе решения следует учитывать факторы производительности инструмента VPN. Например, если маршрутизатор работает уже на пределе возможностей процессора, может добавление туннелей VPN и применение шифрования/дешифрования методы, чтобы сломать всю сеть, потому что этот маршрутизатор не будет управлять простым движением, не говоря уже о VPN. Опыт показал, что лучше всего использовать специальное оборудование для создания VPN, но если средства ограничены, можно обратить внимание на чисто программное решение. Подумайте о том, как мы можем построить VPN.

Брандмауэры большинства производителей поддерживают туннелирование и шифрование данных. Все подобные продукты основаны на том, что движение-это зашифрованный брандмауэром. Модуль шифрования добавляется в программное обеспечение брандмауэра. Недостатком этого метода является зависимость эффективности от оборудования, на котором работает брандмауэр. При использовании брандмауэров на базе ПК надо отметить, что это решение можно использовать только для небольших сетей с небольшим количеством передаваемой информации.

Например, с поддержкой VPN firewall могут быть классифицированы по firewall-1 от Checkpoint Software Technologies. FairWall - 1 использует стандартный подход на основе IPSec для создания VPN. Трафик, который попадает в брандмауэр, значит, и применять правила контроля доступа по умолчанию. FireWall-1 работает с Solaris и Windows NT 4.0.

Еще один способ для создания VPN-создания безопасных каналов маршрутизатора, потому что вся информация из локальной сети, проходит через маршрутизатор.

Пример оборудования для создания VPN с чпу-это оборудование компании Cisco Systems. Начиная с версии IOS 11.3 маршрутизаторы Cisco поддерживают протоколы L2TP и IPSec. Помимо простого шифрования по информации Cisco поддерживает и другие функции VPN, такие как обнаружение туннелей и обмен ключами.

Для повышения производительности маршрутизатора, вы можете использовать дополнительный криптографический модуль esa. Кроме того, компания Cisco System разработала специальный VPN-устройство, которое называется Cisco 1720 VPN Access Router для установки в малых и средних предприятиях и офисов крупных организаций.

Следующий подход для построения VPN являются чисто программные решения. При реализации такого решения используется специализированное

программное обеспечение, которое работает на специальный компьютер и, в большинстве случаев это прокси-сервер. Ваш компьютер с помощью этой программы могут быть размещены за брандмауэром.

Примером этого является обеспечение AltaVista Tunner 97 от Digital. Когда это программное обеспечение используется, клиент подключается к серверу тоннели 97, аутентифицируется на нем и обменивается ключами. Шифрование осуществляется на базе 56 или 128-битных ключей, полученных в процессе подключения. Затем зашифрованные пакеты инкапсулируются в другие IP-пакеты, которые в свою очередь отправляются на сервер. Кроме того, это программное обеспечение создает новые ключи каждые 30 минут, что значительно повышает безопасность соединения.

Положительные характеристики туннеля AltaVista 97 проста в установке и просты в обращении. Минусы этой системы можно считать нестандартную архитектуру (алгоритм обмена семья ключами) и низкую производительность.

Решения на базе сетевой ОС мы рассмотрим пример системы Windows NT компании Microsoft. Для создания VPN Microsoft использует протокол PPTP, который встроен в систему Windows NT. Данное решение является очень привлекательным для организаций, использующих Windows в качестве корпоративной операционной системы. Следует отметить, что стоимость такого решения значительно ниже стоимости прочих решений. В работе VPN на базе Windows NT, которая используется база пользователей NT, который хранится в Primary Domain Controller (PDC). При подключении PPTP server, пользователь аутентифицируется протоколы PAP или CHAP, MS-CHAP. Отправленные пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования пакетов используется пользовательский протокол Microsoft Point-to-Point Encryption с 40 или 128 битным ключом, получаемым в момент установки соединения. Минусы этой системы является отсутствие проверки целостности данных и невозможность смены ключей во время соединения. Положительными моментами являются легкость интеграции с Windows и низкая стоимость.

Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Примером такого решения служит продукт с IPro-VPN компании Radguard. Этот продукт использует шифрование передаваемой информации, способен пропустить поток 100 Мбит/с. IPro-VPN поддерживает протокол IPSec и механизм управления ключами ISAKMP/Oakley. Среди прочего, данное устройство поддерживает средства трансляции сетевых адресов и может заполняться специальная карточка, добавляющей функции брандмауэра4 Методы реализации VPN сетей.

Виртуальная частная сеть базируется на трех методах реализации: туннелирование, шифрование, аутентификация.

1.5 Туннелирование

Туннелирование позволяет передавать данные между двумя точками-туннелем и соединениями, поскольку источник и приемник данных выходят из скрытой части всей сетевой инфраструктуры и располагаются между ними. Транспорт и окружающая среда туннеля, такие как пар, набор пакетов, которые будут использоваться, сетевой протокол на входе в туннель и без изменений, ведущий к выходу. При строительстве тоннеля достаточно соединить два сетевых узла, так что, по условиям эксплуатации их, программное обеспечение как бы соединяется с локальной вычислительной сетью. Однако нельзя забывать, что это, по сути, "лодка" с данными, проходящая через множество промежуточных узлов (маршрутизаторов) открытых, общедоступных сетей.

Эта ситуация чревата двумя проблемами. Первая заключается в том, что она передается по туннелю, информация может быть перехвачена киберпреступниками. Если речь идет о доходах (номера банковских карт, финансовые записи, личная информация), то возникает вполне реальная угроза нарушения, а это уже само по себе немало. Хуже того, злоумышленники имеют возможность изменять передачу данных через туннель данных, так что получатель не сможет проверить их достоверность. Последствия могут быть очень серьезными. Учитывая вышесказанное, можно сделать вывод, что туннель в чистом виде, является удобным дополнением для некоторых видов компьютерных игр, сетевых, и может быть, а может и не подходить для более серьезного тона. Обе эти проблемы решаются с помощью современных средств защиты информации от шифрования. Чтобы предотвратить любые несанкционированные изменения в пакете с данными, находящимися на пути к путевому туннелю, будет использоваться метод цифровой подписи (ЭЦП). Суть этого способа заключается в том, что в каждом из последних пакетов, предусмотренных для дополнительного блока, информация производится по асимметричному криптографическому алгоритму, причем только содержимое пакета и секретный ключ электронной подписи отправителя. С помощью этой информации блок представляет собой пакет ЭЦП, и позволяет осуществлять проверку данных получателем, которому известен открытый ключ электронной подписи отправителя. Осторожность, передаваемая через туннель данных от несанкционированного просмотра, достигается за счет использования мощных алгоритмов шифрования.

Безопасность программного обеспечения-это функция включения VPN. Все данные с клиентского компьютера поступают через Интернет на VPN-сервер. То есть сервер может располагаться на большом расстоянии от клиента, а составляющие пути к сети организации передавать оборудование на большое количество провайдеров. Как вы можете быть уверены, что данные не будут прочитаны или изменены? для этого необходимо применять различные методы аутентификации и шифрования.

Для проверки подлинности пользователей PPTP сможете использовать любой из протоколов, которые будут использоваться для PPTP:

- EAP, или расширяемый протокол аутентификации;

- MSCHAP, или Microsoft challenge Handshake Authentication Protocol (версии 1 и 2);

- CHAP или challenge Handshake Authentication Protocol;

- SPAP, или Shiva Password Authentication Protocol;

- протокол PAP и протокол аутентификации по паролю.

Лучше всего использовать протоколы mschap-v2 и Transport Layer Security (EAP-TLS), как обеспечить взаимную аутентификацию, то есть VPN, сервер и клиент должны быть идентифицированы друг с другом. Для всех остальных протоколов аутентификация клиента выполняется только на сервере.

Хотя PPTP обеспечивает хороший уровень безопасности, но L2TP через IPSec является более безопасным. L2TP через IPSec обеспечивает аутентификацию уровней" пользователь "и" компьютер", а также осуществляет аутентификацию и шифрование данных.

Аутентификация осуществляется либо с помощью открытого текстового пароля, либо по статусу запроса / ответа. При прямом вводе все в порядке. Клиент отправляет пароль. Сервер сравнивает это с эталоном, или запрещает доступ к нему, или говорит "Добро пожаловать". Откройте аутентификацию, то есть почти, и она не всплывет.

Диаграмма запроса/ответа-это гораздо больше продвинута. В общем, похоже на то:

- клиент отправляет запрос на аутентификацию в службу аутентификации;

- на сервере он возвращает случайный ответ (вызов);

- клиент удаляет хэш-код (хешем называется хэш-эффектом, функцией, преобразующей текст таблицы данных произвольной длины в выходную битовую строку фиксированной длины), шифрует ответ и передает его на сервер;

- это делает сервер, и сравнивая результат с клиентом по ответу;

- если зашифрованный ответ совпадает, аутентификация считается успешной;

На первом этапе происходит идентификация VPN-клиента L2TP и сервера по IPSec с использованием локальных учетных данных, которые поступают от продукта и сервиса. Клиент и сервер обмениваются сертификатами для установления безопасного выбора соединения (Ассоциации безопасности). После того, как L2TP (через IPSec) завершает процесс аутентификации на компьютере пользователя, выполняется уровень аутентификации. Для аутентификации вы можете использовать любой из следующих способов, даже PAP, передает идентификатор пользователя и пароль в открытой форме. Это абсолютно безопасно, так как протокол L2TP over IPSec шифрует весь сеанс. Однако выполнение аутентификации пользователя, с помощью MSCHAP, Variety различных ключей шифрования для аутентификации компьютера и пользователя, это может усилить защиту.

Шифрование через PPTP гарантирует, что никто не сможет получить доступ к данным, когда они будут отправлены через Интернет. В настоящее время поддерживаются два метода шифрования:

MPPE, или Microsoft Point-to-Point шифрование файлов совместимо только с MSCHAP (версии 1 и 2);

EAP-TLS, и он будет автоматически установлен на длину ключа шифрования при корректировке настройки между клиентом и сервером.

MPPE поддерживает работу с 40, 56 или 128 битными ключами wep. Более старые операционные системы Windows, с поддержкой шифрования с длиной ключа 40 бит, и поэтому, в смешанной среде Windows, вам нужно выбрать минимальную длину ключа.

PPTP изменяет значение ключа шифрования для каждого входящего пакета. Протокол MMPE был разработан для двухточечных каналов связи, в которых пакеты передаются правильно, и потеря данных очень мала. В этом случае значение ключа для новой службы зависит от результатов предыдущего пакета. Во время создания виртуальных сетей с помощью файлообменных сетей, а эти сроки и условия должны контролироваться не представляется возможным, так как пакеты данных часто попадают к получателю, а не в том порядке, в котором они были отправлены. Поэтому PPTP использует а для изменения ключа по умолчанию для шифрования порядкового номера пакета. Это позволяет запускать а дешифрациь, независимо от ранее загруженных пакетов.

Оба они используются как в Microsoft Windows, так и за ее пределами (П. Аллах., Лицензия для VPN анализ задания может значительно отличаться. В НТ (и отвечает за поиск).

Таким образом, связь под названием "воронка + контроль + шифрование" позволяет передавать данные между двумя точками через общедоступную сеть, устройство работает в частной (локальной) сети. Другими словами, рассматриваемые как инструменты, они позволят вам создать виртуальную частную сеть.

Дополнительным приятным эффектом, при наличии VPN-соединения, является возможность (и необходимость) использования подзаконных актов расчетной системы к локальной сети.

Реализация виртуальной частной сети, на практике, заключается в следующем. Был определен локальный офис сети компании, VPN-сервер. Удаленный пользователь или маршрутизатор, если две службы связаны с использованием программного обеспечения клиента VPN, то начинается процесс подключения к серверу. Аутентификация пользователя осуществляется на первом этапе установления VPN-соединения. В том случае, если сертификат нужен, наступает второй этап-между клиентом и сервером, он уже появился в мире элементов безопасности. После этого осуществляется управление VPN-соединением, которое предусматривает обмен информацией между клиентом и сервером, в формате, когда каждый пакет данных проходит

через процесс шифрования/дешифрования, а также проверку целостности данных для идентификации.

Основной проблемой VPN-сетей стало отсутствие продукта и установления стандарта, а также зашифрованного обмена информацией. Эти стандарты все еще находятся в стадии разработки, и поэтому продукты разных производителей могут быть не VPN-соединением, а автоматическим обменом ключами. Этот вопрос связан с замедлением темпов расширения сети VPN, поскольку трудно сделать множество различных компаний для использования продуктов одного и того же производителя, но из-за того, что это сложный процесс унификации сетей компаний-партнеров, т. н. экстрасети и сети.

В зависимости от расстояния между системами абонентскими и компьютерными сетями они делятся на общий, территориальный и локальный уровни. Существуют универсальные и специализированные сети.

Иерархию компьютерной сети можно сформулировать следующим образом (рисунок 1.2).

Рисунок 1.2 - Иерархия компьютерных сетей

1.7 Понятие "туннеля" при передаче данных в сетях

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (такой канал называется "туннелем", а технология его создания называется "туннелированием"). Вся информация передается по туннелю в зашифрованном виде (рисунок 1.3).

Рисунок 1.3 - СхемаVPN-туннелирования

Одной из основных функций VPN-брокера является пакетный фильтр. Фильтрация пакетов осуществляется с помощью VPN-агента, настройки которого в целом являются политикой безопасности виртуальной частной сети. Для повышения безопасности виртуальных частных сетей в туннелях используются брандмауэры, а также инструменты (фильтры).

VPN-или быть сделанным из роли VPN-шлюзов. Шлюз безопасности — VPN-это сетевое устройство, которое было подключено к двум сетям-Wan и lan-соединениям, и должно выполнять функции шифрования и аутентификации компьютеров, расположенных за этим экраном. VPN-портал может быть реализован как отдельное аппаратное устройство, в частности из решений, а также в виде брандмауэра или маршрутизатора, расширенного возможностями VPN.

Сетевое подключение к шлюзу безопасности VPN, по-видимому, клиент находится за пределами этой сети, например линии, хотя на самом деле это открытая сеть с включенными пакетами. VPN-шлюз по безопасности адреса со стороны внешней сети определяет адрес входящего Package пакета. Внутренний адрес-это адрес хоста, который находится за ним. Шлюз безопасности VPN может работать на маршрутизаторе, брандмауэре и т. д.

Feature особенность заключается в том, что эта технология позволяет шифровать исходный пакет целиком, вместе с заголовком, а не только данные в поле. Исходный пакет зашифровывает полностью, вместе с заголовком и зашифрованным пакетом помещается внутри другого внешнего пакета, чтобы открыть заголовок. Передача данных из "опасной" сети и открытых участков внешнего пакета также используется при появлении внешнего пакета, в точке его защитного канала они удаляют внутренний пакет, декодирование и использование заголовка для будущей передачи, даже в открытом виде по сетке, не требует защиты (рисунок 1.4).

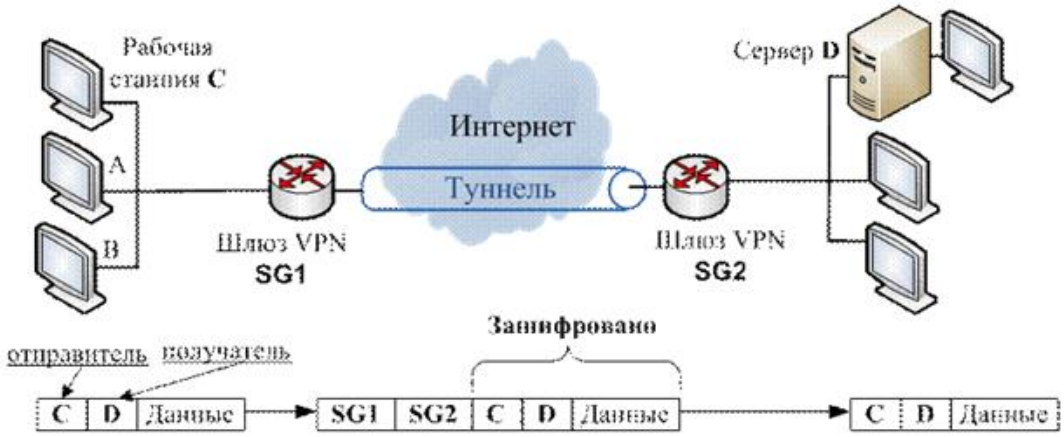

Рисунок 1.4 - Организация туннеля VPN

При этом для внешних пакетов используются адреса пограничных маршрутизаторов (VPN-шлюзов), установленных в этих двух точках, а внутренние адреса конечных узлов содержатся во внутренних пакетах в защищённом виде (рисунок 1.5).

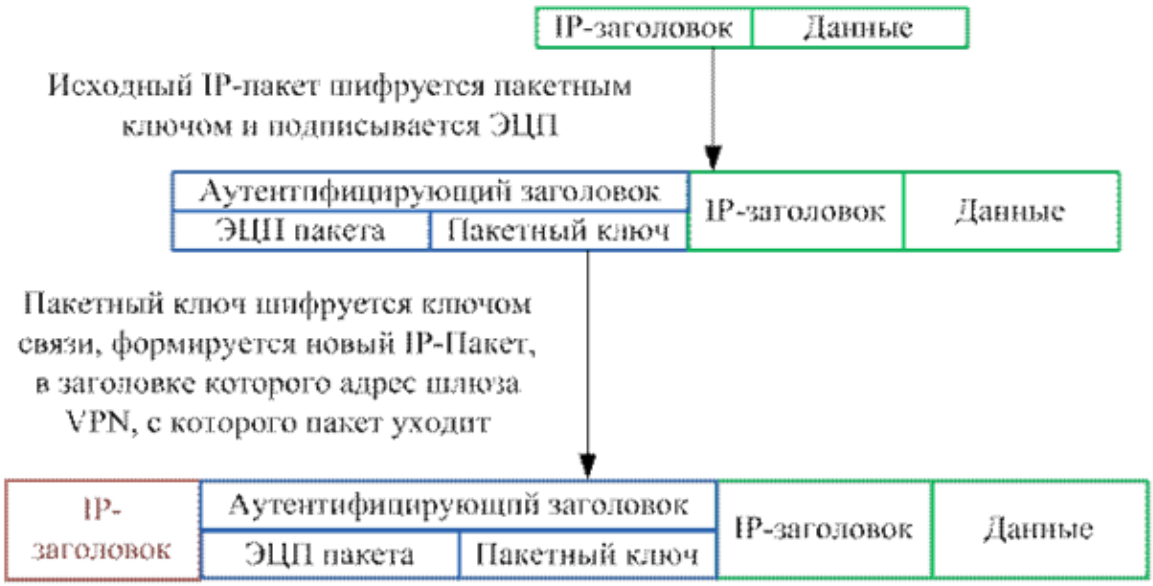

Рисунок 1.5 - Туннелирование пакетов

1.8 Виды архитектуры VPN-сетей

С помощью схемы (рис. 6) осуществляется удаленный доступ отдельно взятых сотрудников к корпоративной сети организации через общедоступную сеть. Удаленные клиенты могут работать на дому, либо, используя переносной компьютер, из любого места планеты, где есть доступ к всемирной паутине.

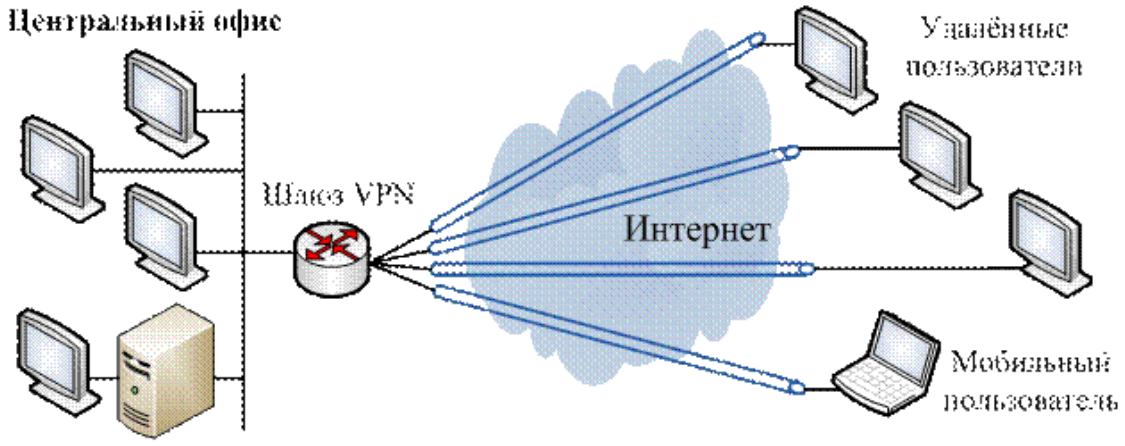

Рисунок 1.6 - VPN с удалённым доступом

Существует подключение к публичной сети территориально распределенных филиалов. Этот метод называется интрасеть VPN. Таким образом, его не рекомендуется использовать для общих филиалов, а также для мобильных сервисов, к которым вы будете иметь доступ на ресурсе "родительской" компании, а также без проблем и для обмена информацией друг с другом (рисунок 1.7).

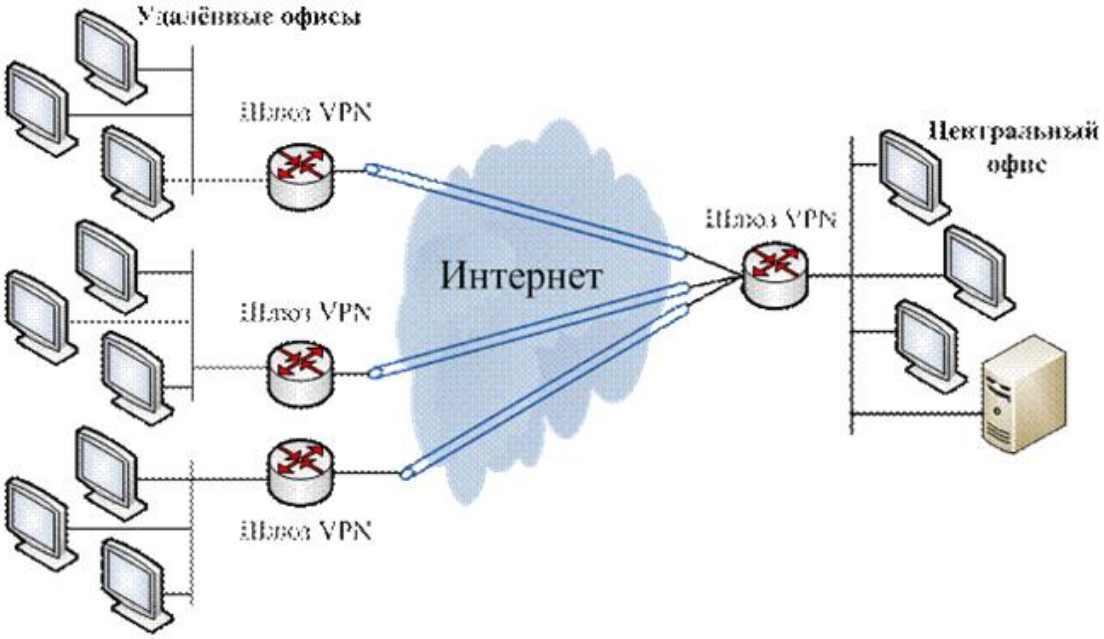

Рисунок 1.7 - Intranet VPN

Межкорпоративные VPN- это так называемый Extranet VPN, когда через безопасные каналы доступа предоставляется доступ для клиентов или партнёров организации. Набирает широкое распространение в связи с популярностью электронной коммерции.

В этом случае удаленные клиенты (партнеры) будут сокращать возможности использования корпоративной сети, а фактически это будет ограниченный доступ к таким ресурсам для компании, который необходим при работе с клиентами, например, веб-страница, с коммерческими предложениями, а VPN используется, в данном случае, для того, чтобы безопасно отправлять конфиденциальные (данные рисунок 1.8).

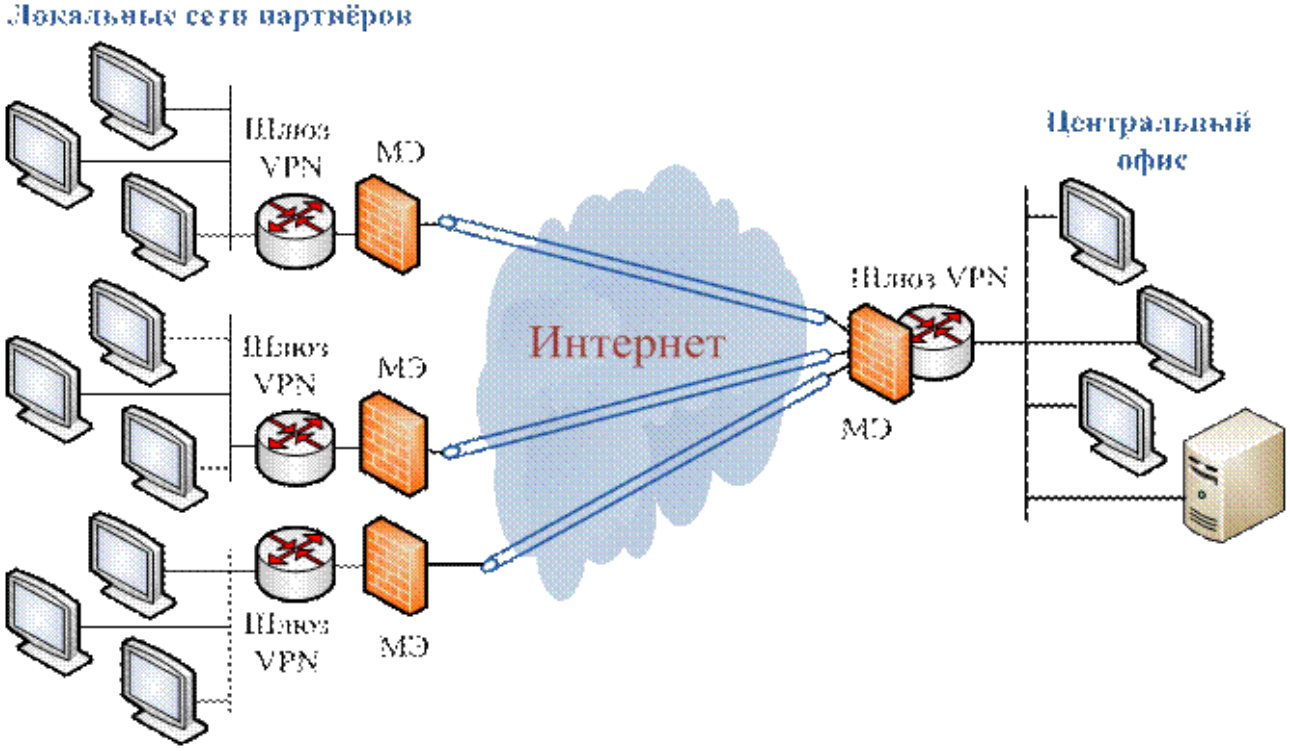

Рисунок 1.8 - Extranet VPN

На рисунке 8 из VPN-шлюзов-даже у меня-появился брандмауэр-и он появился. Брандмауэры (фильтры) обеспечивают контроль над передаваемым контентом (вирусами и другими внешними атаками). Для меня это" забор "вокруг сети, который препятствует проникновению в нее злоумышленников, а в то время как VPN-это" машина для побега", которая защищает ценности и при удалении на внешнюю сторону забора. Поэтому необходимо использовать два решения для обеспечения необходимого уровня безопасности информационных ресурсов. Часто для меня и функция VPN объединяются в одном устройстве.

2 Организация архитектуры VPN-сетей

MPLS (MultiProtocol Label Switching) - это технология быстрой коммутации пакетов в сетях многопротокольных, основанная на использовании меток. Кабельные компании еще не были разработаны и продаются как способ построения высокоскоростных интернет-практик, однако, что сфера применения не ограничивается протоколом IP, а относится к пропускной способности любого сетевого протокола маршрутизируемого.

Традиционно требования и технология "в воздухе" имеют высокую пропускную способность, значение задержки и хорошую гибкость. Однако нынешняя рыночная ситуация диктует новые правила игры. Теперь для сети вашего провайдера услуг недостаточно просто обеспечить доступ к интернет-магистрали. Модифицированный пользователь должен также включать доступ к встроенным сетевым сервисам и организации виртуальных частных сетей (VPN), а также множество других интеллектуальных функций. Увеличение спроса на большее количество услуг, которые будут продаваться через легкий доступ IP, обещание сделать интернет-провайдеров сверх доходов.

Для решения задач вызова и развития архитектуры кабельных компаний не требуется, что предусматривает построение сети, обладающей практически бесконечными масштабируемыми возможностями, а также повышенным трафиком, скоростью обработки и беспрецедентной гибкостью в плане организации дополнительных услуг. Кроме того, у кабельных компаний нет технологии, позволяющей интегрировать IP и ATM сети, поставщики услуг смогут не только сэкономить средства, вложенные в оборудование асинхронной передачи, но и устранить избыточное распределение выгод по этим протоколам.

За разработку архитектуры, которую кабельные компании не делают, отвечает одноименная рабочая группа, которая входит в группу маршрутизации IETF. Активное участие в мероприятиях приняли представители крупнейших поставщиков сетевых решений и оборудования. Эта архитектура была увеличена от ссылки на данные системы, предложенной Cisco Systems, однако некоторые идеи были перенесены на параллельную технологию IP-коммутации, разработанную Ipsilon, и продукт IBM Aris. У кабельных компаний дизайн не собрал самых удачных элементов из всех мероприятий, и вскоре он будет преобразован в стандартный интернет-благодаря усилиям IETF, а сами компании не заинтересованы в быстром продвижении технологии на рынок.

Классическая технология VPN позволяет осуществлять передачу информации именно через муравьиные туннели. У кабельных компаний нет VPN, нет шифрования. Пакеты, чтобы "спрятать" от посторонних глаз, так как они перевозятся на время, кабельные компании не ставят меток. Трафик определенных символов в доступных только для чтения маршрутизаторах LSR (Label Switch routers) расположен на отмеченном следе. Обычный способ IP-маршрутизации кабельных компаний, не имеющих своей сети, не применяется

- трафик маршрутизируется только по следам меток. Никому не возбраняется дальнейшее использование кабельными компаниями не самого пакета, если это необходимо (рисунок 2.1).

Кабельные компании не имеют VPN-инфраструктуры, включающей программное обеспечение и построение распределенного клиента в IP-сети внутри VPN. То есть VPN обеспечивается обменом пакетами между IP-сетями.

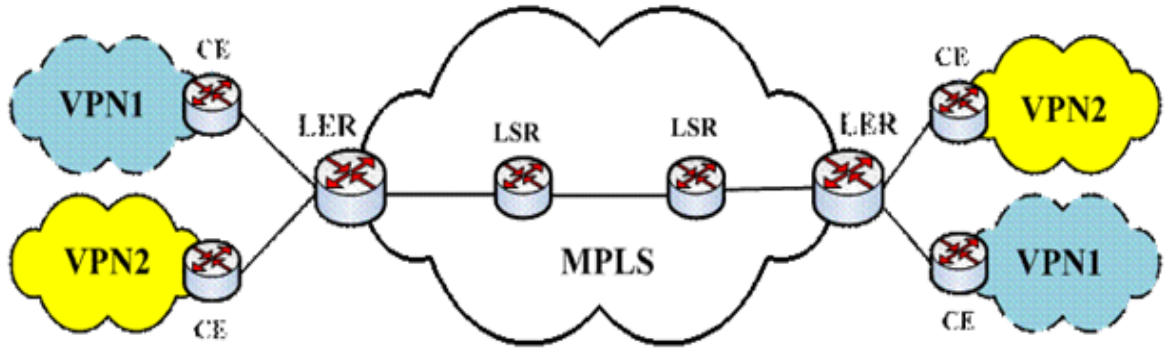

Рисунок 2.1 - Сеть MPLSVPN

В терминах кабельных компаний не существует VPN, особенно соединение CE, именуемое веб-сайтом. Каждая веб-страница - это отдельная клиентская подсеть, устройство в структуре VPN.

Необходимым условием в сети VPN, является противодействие безудержному производству клиентского трафика данных из сети VPN и его смешиванию с потоками данных из других сетей, и, в этом смысле, кабельные компании не используют технологию VPN, отвечающую этим требованиям.

Преимуществом данной технологии является высокая скорость маршрутизации IP-пакетов по сети за счет сокращения времени обработки information информации. Полностью отделенные друг от друга виртуальные корпоративные сети. На базе этой сети работают некоторые поставщики услуг по IP-телефонии, видеопередаче, в зарубежной стране по мониторингу, обучению на работе, виртуальной отчетности, системам видеокон-ференцсвязи, а также по заказу и бронированию железнодорожных и авиа билетов, с дистанционным управлением для контроля потребления воды и тепла в помещениях компании и многое другое.

Кабельные компании не имеют VPN-сети, которые можно разделить на две области: IP-клиент в сети и линия обслуживания. Классические кабельные компании не имеют VPN, чтобы план состоял из следующих компонентов: ограничение на маршрутизаторы в сервисе провайдера LER, (Label Edge routers), направленном на оборудование CE. В рамках грозовых облаков кабельные компании не используют маршрутизаторы в сервисе провайдера, который называется label routers (Label switch in the routers) - LSR непрерывно преобразуется в основной, основанный на том, что кабельные компании не используют метки. Перед отправкой трафика в кабельные компании делают не Сеть, а маршрутизаторы ler, первыми организующие LSP (dial-up Route-tags), в

ходе работы кабельных компаний не имеют сети дистанционного управления LER.

Распределение трафика VPN, в частности VRF ads (таблица VPN, маршрутизации и пересылки), используется для указания взаимосвязи различных пакетов VPN. VPN-теги, которые прикрепляются к CE CE и используются для маршрутизации роутерами ler. В результате передача данных по каналу path (LSP) настраивается в кабельных компаниях, не имеющих сети. Принцип работы сети MPLS VPN можно понять (рисунок 2.2).

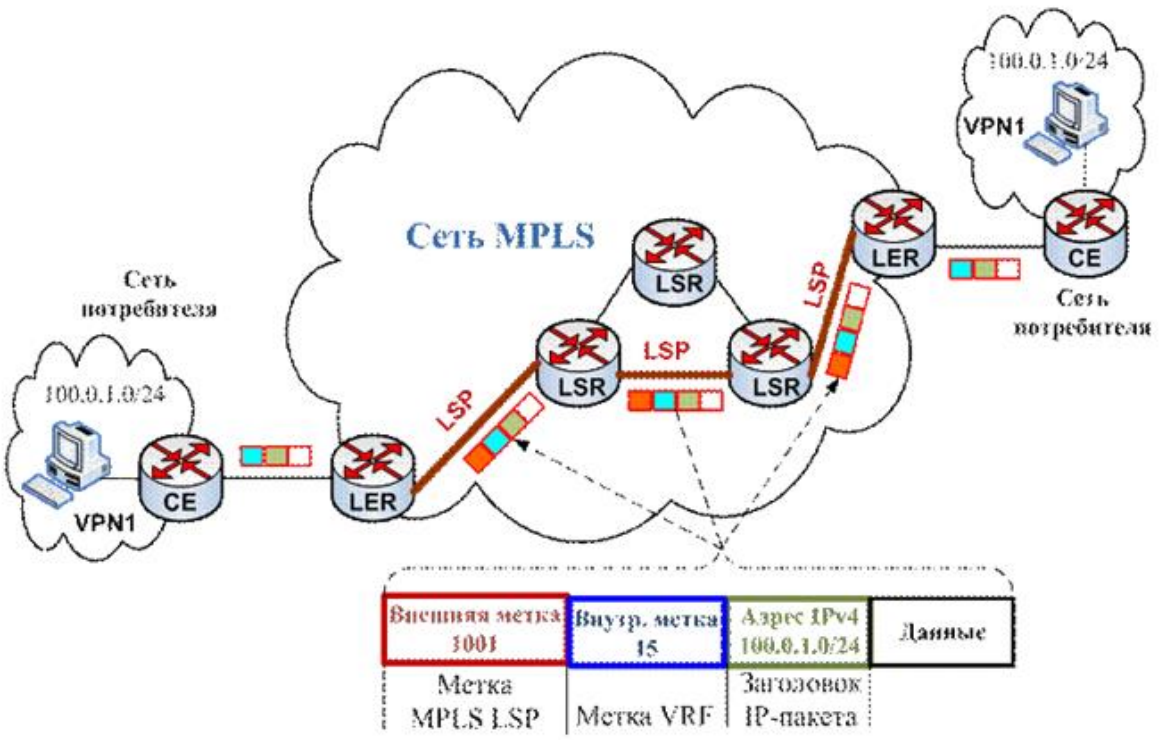

Рисунок 2.2 - Схема передачи данных в сети MPLSVPN

Слева и справа появляются два веб-сайта в одном и том же VPN1. На компьютере веб-страница отправляет данные на ваш компьютер в том же VPN1, который находится на веб-сайте. Соответствующий IP-адрес, обратитесь к дейтаграмме. Дейтаграмма, вы можете получить маршрутизатор ler, который распознал, что правильный адрес vpn1, и установить их в соответствующую метку Intra-VRF.

На метке указывается не только номер VRF (этикетка 15), но и информация об информации, подлежащей передаче в LSP = 1001. Таким образом, определяется передача данных по каналу маршрутизатора LER, который находится в положении введения. Передача производится через кабельную компанию, а не через LSP, и дейтаграмма вы получаете два ярлыка-кабель, причем компания не имеет сети, а сеть VPN, соответственно. Web-site-ler-left-VRF-owner был удален, и данные-это простой заголовок, дейтаграммы, VPN и IPv4-адрес.

Таким образом, технология VPN в современной сети передачи данных использует ту же философию для среднего имени, которая, как правило, имеет полную IP-технологию.

2.1 Элементы архитектуры.

Метка-это короткий идентификатор фиксированной длины, который определяет класс FEC. С помощью пакета этикеток значение определяется принадлежностью к определенной категории, каждый раз набираемой кусками.

Как ранее было описано, цель должна быть уникальной только в контексте отношений между каждой парой логически смежных LSR. Таким образом, концепция заключается в том, что вы можете использовать LSR для связи с различными соседними маршрутизаторами, если у вас есть возможность определить, какой из них входит в пакет этого характера. Другими словами, в соединениях "точка-точка" можно использовать набор меток для окружающей среды, для окружающей среды, при этом все больше и больше доступа требуется и набор меток для блока или всего блока. В реальном выражении угроза истощения этого района отметок очень маловероятна.

Прежде чем можно активировать пакет, необходимо сразу же обозначить определенный способ шифрования. В случае использования протокола IP необходимо поместить в специальный "тонкий" заголовок пакета, инкапсулирующего IP-адрес. В других случаях метка хранится в заголовке уровня протокола или кодируется как конкретное значение VPI/VCI (в сети ATM). Чтобы добавить протокол IPv6, этикетку упаковки можно поместить в поле идентификатор курса.

В рамках архитектуры MPLS вместе с пакетом разрешено передавать не одну метку, а целый их стек. Strip теги, которые будут определены как Push/pop результат. Результат переноса, определенный только в верхней части стека, является индикатором, в нижней части сам сообщается в четком, еще до начала операции, штурме сверху. Такой подход позволяет создать потоковую иерархию в кабельных компаниях, не имеющих сети и организации Break взлома. Стек состоит из случайного числа элементов, каждый из которых имеет длину 32 бита: 20 битов-это, по сути, этикетка, 8-это сведенные вместе под упаковкой счетчики времени жизни, один показывает склад раньше, и все три из следующих не должны использоваться. Будьте счастливы, что вы можете получить его за любую цену, за исключением пары паровых (рисунок 2.3).

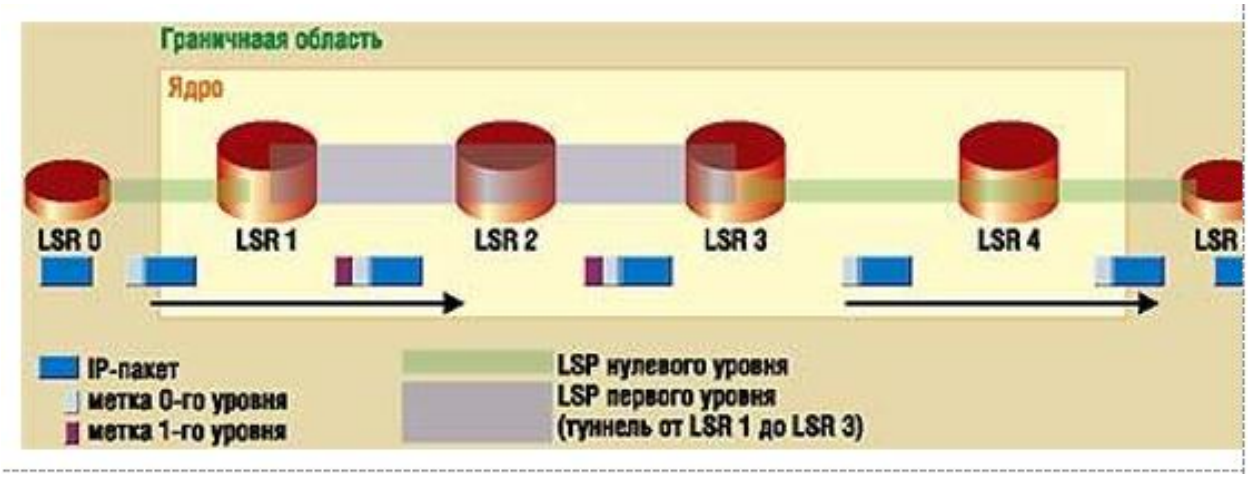

Рисунок 2.3 - Компоненты коммутируемого соединения

Прохождение пути (LSR) уровень состоит из последующих участков, что происходит с именования этого слоя (рис. 12). Например, LSR нулевой уровень, который проходит через устройства LSR 0, 1 LSR, LSR 3, LSR 4 и LSR 5. При этом LSR 0 и LSR 5 являются соответственно входными (входными) и выходными (домашними) маршрутизаторами на нулевом уровне дороги. LSR 1 и LSR 3 играли одинаковую роль для LSR первого уровня, первый из них производил компании по добавлению тегов в стек,а второй-по атаке. В любом сегменте LSR можно выделить верхний и нижний LSR по отношению к трафику. Например, раздел" LSR 4-LSR 5 " маршрутизатора будет верхним и нижним.

2.3 Построение коммутируемого маршрута

Рассмотрим, как система MPLS автоматически создает путь LSP в простейшем случае — с помощью протокола LDP. Архитектура MPLS не требует обязательного применения LDP, однако, в отличие от других возможных вариантов, он наиболее близок к окончательной стандартизации.

Во-первых, по многоадресным сообщениям UDP, меняя маршрутизаторы, определяет "соседние страны" (смежность) в соответствии с протоколом ldp. Кроме того, по близости уровня канала передачи данных, полезности ldp, можно определить связь между "логически смежными" LSR,не принадлежащими ни к одному каналу. Для этого необходимо провести транспортный тоннель. На котором он установлен, утилита ldp открывает транспортную связь для обсуждения между участниками по этому поводу. В связи с этим он передал требования к установке соединения и информацию о соединении с самим собой. Кроме того, участникам совещания может понадобиться проверить эффективность работы друг друга, вы отправляете текстовое сообщение (keepalive message) (рисунок 2.4).

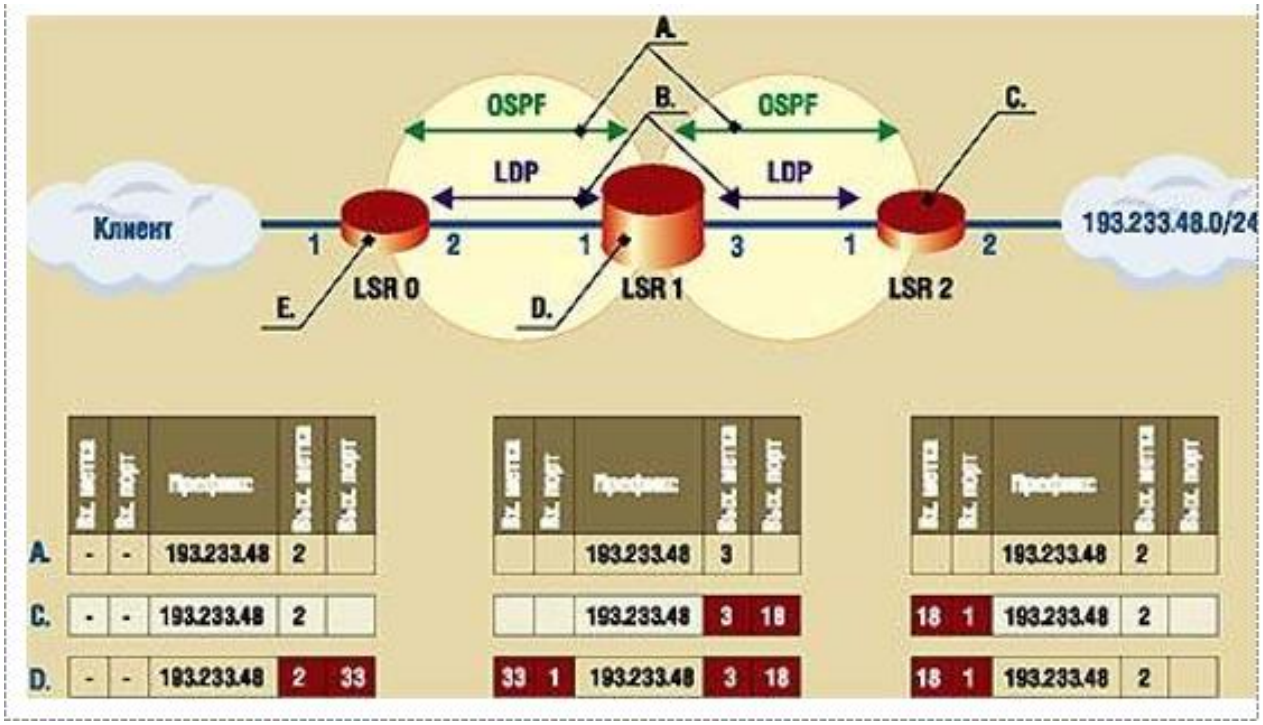

Рисунок 2.4 - Построение коммутируемого пути по протоколу LDP

Можно видеть, как таблица символов должна быть заполнена протоколом ldp (рис. 13). Предположим, что вы должны быть в правильном направлении, распределение LSP отмечает спонтанное расширение информации о соединении.

В процессе работы ни одна из кабельных компаний не располагает сетевыми устройствами и строит базу данных information информации, когда действует какой — либо из текущих протоколов маршрутизации (Bar-OSPF). В фазе Б LSR-маршрутизаторы реализуют процедуру выбора своего оборудования и для установки их в обсуждениях в ЛДП являются новыми.

Из (фазы с) LSR 2, на основе анализа его таблиц маршрутизации показывают, что именно LSR в выходные дни, на дороге, которая ведет к IP-сети, 193.233.48.0. Тогда LSR 2, связанный с пакетом FEC класса а с адресом приемника, является соответствующим префиксу этой сети и присваивает этому классу случайный выбор в значении счета — в данном случае 18. Есть ссылка, протокол ldp, сообщаемый сверху-маршрутизатор LSR (LSR 1) и то, что находится внизу, Network сеть с префиксом 193.233.48, у вас будет отметка 18. LSR 1 помещает это значение в выходные значения коробки на столе.

В ходе фазы LSR 1, устройство, которому известна метка значения тока, специально изготовлено для требования 193.233.48, учитывая его важность, маркировки с помощью FEC и отчета в верхней части соседа (LSR 0)для подключения. Теперь LSR до 0 и записывает информацию в таблицу. В конце этого процесса он готов передать пакет от "клиента", сеть - это сетевой адрес 193.233.48.0, то есть LSP, конечно.

Спецификация Category-FEC может содержать несколько компонентов, каждый из которых определяет набор пакетов, соответствующих этой

категории. На сегодняшний день установлены два бита FEC: адрес хоста и префиксный адрес. Пакет классифицируется как часть этой группы FEC, если адрес получателя точно совпадает с местоположением, адресом, объектом или имеет максимальное совпадение с префиксом адресным. В нашем примере сайт-LSR 0 осуществляет в течение всего времени передачи, продажи пакетов, которые мы будем приходить к нему, из сети к клиенту, и, если адрес его отправителя совпадает с префиксом 193.233.48), придавая ему метку пакета 33, он отправляет ее через интерфейс 2.

Маршрутизация выполняется через слой 3, сайты, а затем идет преобразование пакета (переписывание L2 и так далее).

Так вот, кабельные компании делают вещи не по IP-адресам, а по специально созданным персонажам. То есть для каждого маршрута кабельные компании не создают отдельную метку, а значит, четко определено, что это именно так, нет необходимости искать следующий переход, окружение и так далее, нам просто нужна метка и ничего больше.

Таким образом, скорость обработки данных увеличивается, однако, как показывает практика, эта скорость время от времени увеличивается, как и обежалось, но намного меньше, так что все работают через CEF.

То есть, если необходимо внедрять кабельные компании не только для улучшения ваших показателей работы, то это того не стоит.

Таким образом, можно выделить, то на чем основывается MPLS:

- IP-адрес роутинге и CEF;
- Сорвардинг происходит со специально созданными персонажами;
- Кабельные компании обычно не помечают метку, указывающую на целевую сеть. Каждая сторона может привести к себе такой параметр как QOS;
- кабельные компании не полагаются на используемый протокол IGP;

Исходя из вышесказанного, маршрутизатор состоит из плоскости управления и плоскости данных, которые в свою очередь состоят из протокола маршрутизации, ребра и FIB, Adj-таблицы.

С использованием кабельных компаний этого не происходит, это немного расширяется.

При управлении самолетом был добавлен протокол для обеспечения возможности совместного использования протокола обмена метками (ldp или TDP), а затем он был помещен в информационную базу меток (LIB).

Затем он передается на плоскость данных, которая создается в KES и называется таблицей переадресации меток (LFIB).

И происходит коммутация пакетов на основе меток.

В целом он очень похож на IP-переадресацию и IP-маршрутизацию, только это даже дополнение, в календарном формате.

Если это графическое изображение, то оно будет (рисунок 2.5).

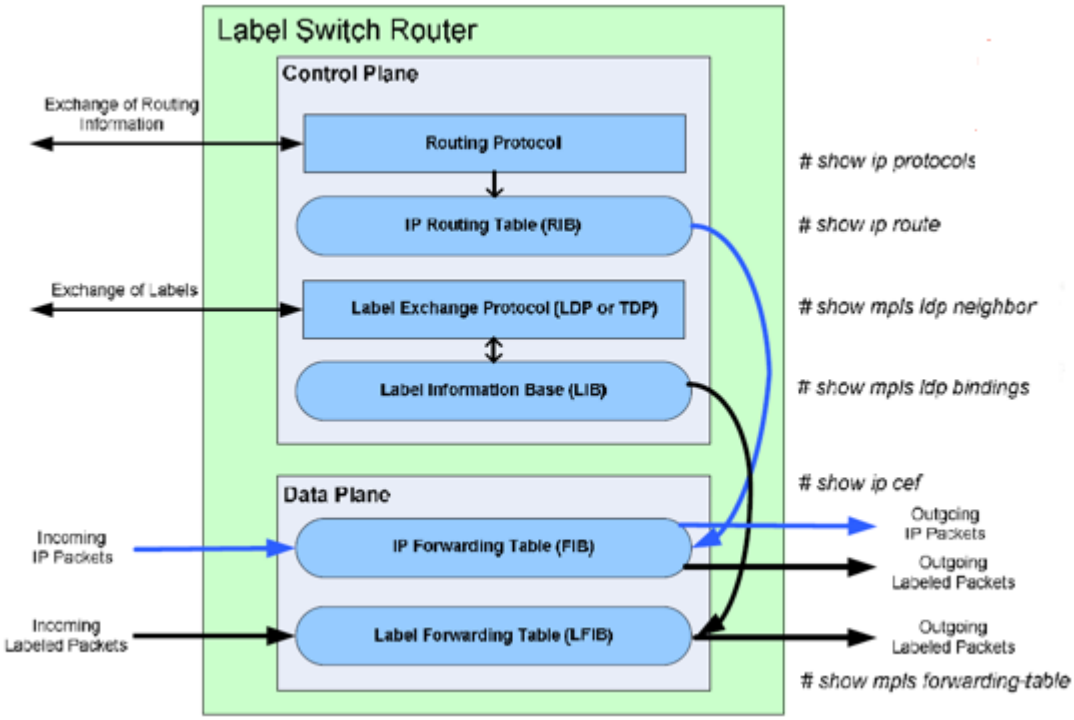

Рисунок 2.5 - Control Plane и Data Plane

Управление самолетом, на основе протокола маршрутизации, создает таблицу ребер, а затем, на основе этой таблицы-протокол обмена метками протокола, который генерирует метку для маршруток, поступивших из IGP, и действия этих символов, с соседними маршрутизаторами.

Кроме того, необходимо создать информационную базу меток, состоящую из сети меток. Теги передаются соседям, используя один из протоколов ldp (стандартный протокол), TDP (протокол Cisco, старый) или через таблицу.

Далее создается плоскость данных, и LFIB содержит метку и интерфейс, через который был выпущен пакет.

Плоскость данных не зависит от того, какое распределение направляющих на этикетке будет использоваться. Плоскость данных идет к очень простому процессу, подставленние ввода символа Кеши.

У кабельных компаний нет сети есть два типа маршрутизаторов:

Метка switch Router (LSR) на всех интерфейсах кабельных компаний осуществлять не приходится.

Основной целью такой маршрутизации является обмен знаками, среди прочего, LSR роутерами, и передача символов пакета.

- край LSR во всех интерфейсах кабельных компаний осуществлять не придется. Только этот маршрутизатор можно классифицировать как Router маршрутизатор кабельных компаний не работает. То есть маршрутизатор (роутер) отправляет пакет со знаками для кабельных компаний не работает, а IP-пакет для внешних кабельных компаний не работает.

Существует такая вещь, как путь с коммутацией LSP-меток, это совокупность LSR, чтобы пакет был от начала до конца. В качестве эквивалента путешествия, которое запомнилось рядом со столом.

Для каждой категории трафика был создан LSP. Этот класс трафика в кабельных компаниях не называют классом эквивалентности пересылки или FEC.

FEC - это группа пакетов, которые должны транспортироваться одним и тем же способом, они имеют один и тот же LSP и один и тот же адрес назначения. Также в ТЭК могут быть созданы и другие критерии.

Графика всех из них может быть отображена (рисунок 2.6).

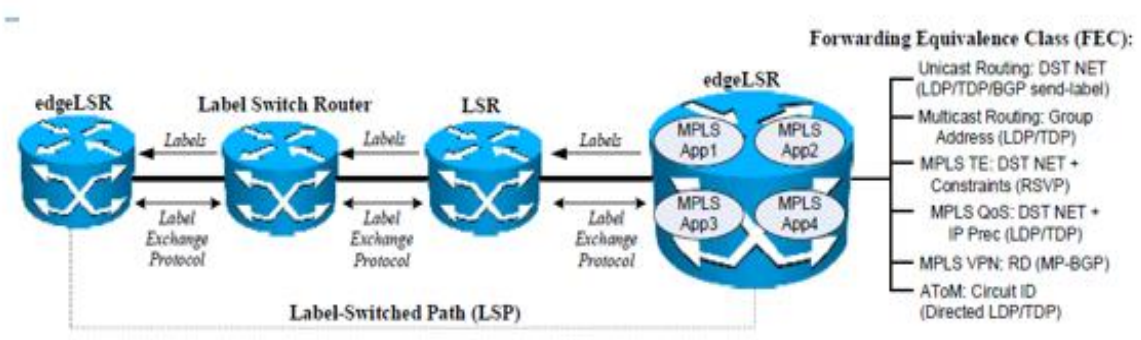

Рисунок 2.6 - Forwarding Equivalence Class или FEC.

На рисунке изображены и различные приложения (FEC) и LSR и eLSR, и что такое LSP (рисунок 2.7).

Рисунок 2.7 – Метка

а) Метка занимает фиксированное число байт, 4 байта.
б) 20 бит выделено под саму метку (просто число).
в) 3 бита выделено под QOS (IP Prec).
г) 1 бит для групповых меток (узнаем чуть позже).
д) и 8 бит — TTL (который может быть свой, а может браться из IP).

Коммутация MPLS может быть двумя способами:

1. frame-Mode — наша метка инкапсулируется в фрейм. Вставка метки происходит между заголовком Layer 2 и Layer 3;
2. cell-mode — применяется в сетях ATM, тут не используется 4 байтовая метка, а вместо них используются vpi/vci (рисунок 2.8).

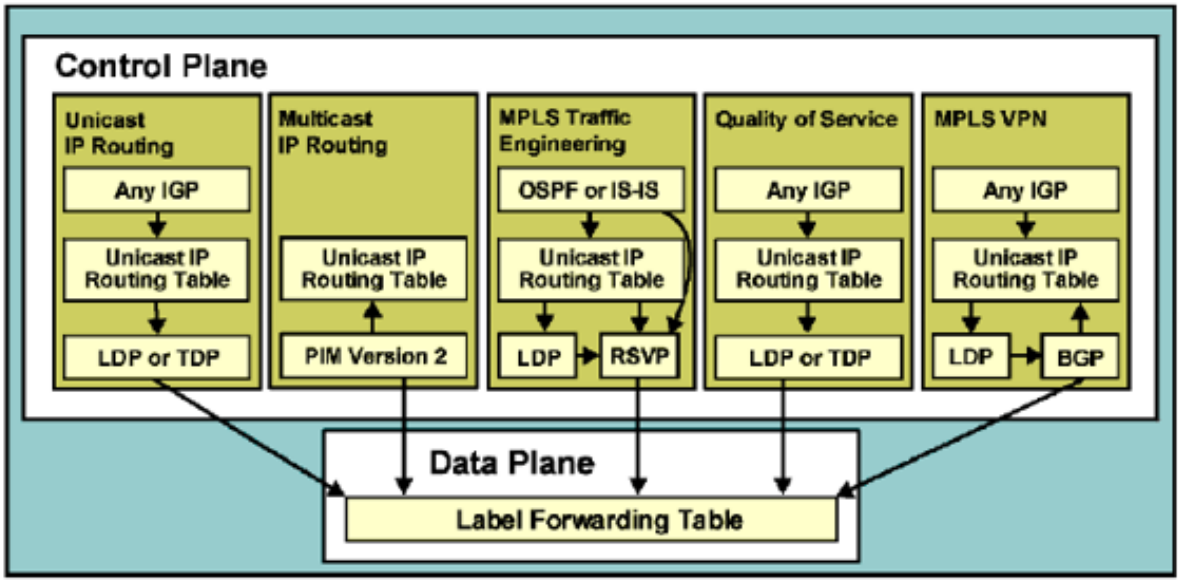

Рисунок 2.8 - Основной MPLS, построенный на unicast ip routing.

Здесь FEC является целевой сетью. Это приложение для внедрения в кабельных компаниях не делают, не рекомендуется. Оказывается, кабельных компаний нет, ибо кабельных компаний нет и в помине. Да, это немного сеть, но разгоняться она уже не будет нужна, и нового сервиса там не будет.
Многоадресная Ip-маршрутизация, в этом приложении FEC будет находиться в пакете с групповым адресом, с этой технологией не рекомендуется использовать в качестве IP-многоадресной рассылки то же самое, а также в отношении этих вопросов.

У кабельных компаний нет транспортной инженерии, ТЭК является целью сети, но есть еще добавленная стоимость, есть вариант, например программный ресурс. Например, нужно построить дорогу не только как стандартную, в кратчайший срок от истока до пункта назначения, а то, что нужно сделать с этим каналом, сказано в 8мегабит, причем, исходя из того, что он будет построен в срок. В этом случае протокол IGP может работать только на OSPF или Is-is.

В кабельных компаниях QOS не FEC зависит от целевой сети, а также от класса обслуживания (COS). То есть получается сложная Одноадресная IP-маршрутизация собственного QOS.

Кабельные компании L3 не используют VPN-это высоко масштабируемое приложение, которое поддерживает такие интернет-сервисы, как: несколько получателей, QOS, Телефония. Вот, фик Бельфор это VPN автоматически. Технология довольно велика, и ему придется рассмотреть ее в деталях, причем в будущем.

L2 кабельные компании не делают VPN или какой-либо транспорт через кабельные компании не делают-L2 VPN, со всеми недостатками и достатками. Для работы кабельных компаний не нужно сначала выявлять кабельных компаний, не имеющих соседей, и устанавливать с ними связь.

Все это происходило и с использованием протокола распределения ldp-меток.

В начале все кабельные компании не взаимодействуют, посылается приветственное сообщение (каждые 5 секунд). Существует сообщение, отправленное UDP на шину протокола к порту 646.

Кроме того, сосед получил это сообщение, пытаясь организовать сеанс. Сеанс устанавливается по протоколу TCP, а порт остается прежним — 646. Протокол TDP использует порт 711.

Есть сообщение, отправленное всем роутерам The мультикасту: 224.0.0.2.

Идентификатор LPD, состоящий из 6-байтового до 4-байтового набора идентификатора маршрутизатора, а 2-й до последнего был полем тега.

Существует два вида меток :

– per-interface label space-это когда метки генерируются в зависимости от типа интерфейса, T the.It есть. для каждого интерфейса на каждой стороне.

Пространство меток для каждой платформы, если метка создается на маршрутизаторе, то есть для каждого листа одной и той же метки. Интерфейс может быть использоватьс, например, что у нас есть ATM-ссылки.

Ниже он описывается как торговля этими ярлыками области:

LSR устанавливает ldp-соединение с сообществом в каждом пространстве метки. Таким образом, на платформе только одно соединение ldp с сообществом является подходящим, даже если существует много параллельных линков между LSR.

Например, LPD IDS: 10.1.0.1: 0, "0 "указывает на то, что платформа используется," 1 " указывает на то, что интерфейс At используется.

Сосед:

- Прямое подключение-то есть когда у соседа есть связь с маршрутизатором через L2.

- Не-непосредственно-связанный-когда он находится между соседями, а не соединение L2. Мы проводим аналогию со столом, когда используем multihop.

Нет надобности напрямую связываться с тем, что сработало, вы должны сообщить об этом через команду: кабельные компании не участвуют, это не neighbourpor {vrf} {ip}.

То есть было упомянуто, что нам нужно пробросить LDP-Session в соответствующем IP-адресе, или VRF.

Там, где это может быть и не нужно;

Кабельные компании делают не быструю стрелку-это Fizza, которая генерируется бекапный LSP, а в случае отказа Первого из них и бекапный немедленно приступают к работе;

Кабельные компании не останавливают Фрахт-NSF) - в случае отказа самолета управления он продолжается;

Кабельные компании не используют ldp-защиту сеансов-это часть быстрой переадресации;

Никаких перевозок по кабелю компании не делают (Атом).

Привет это включено по умолчанию, заходите между разными соседями по множеству различных способов, например, между прямыми соседями, по умолчанию, выполняется каждые 5 секунд, а время удержания = 15, Между не-непосредственно-до 60 секунд времени удержания = 180.

Рекомендуется, чтобы все ссылки вы строили петлю назад, и не только кабельные компании этого не делают, но и это тоже BGP, OSPF и так далее.
Еще один очень важный момент-сеанс TCP запускается на маршрутизаторе, который имеет несколько ldp-идентификаторов сообщества.

После того, как собрание было установлено, приветственное сообщение отправляется и keepalive, по умолчанию, keepalive = 60 секунд; если после 180 секунд и не будет совместно использоваться keepalive, то соседство будет нарушено.

Чтобы изменить таймеры, вы можете использовать команду: кабельные компании не делают ldp discovery {Hello / targeted-hello} {holdtime / interval} XX секунд

Исходя из этого, следует, что приветственные сообщения обмениваются через соединение, а keepalive обменивается только с ближайшим соседом (рисунок 2.9).

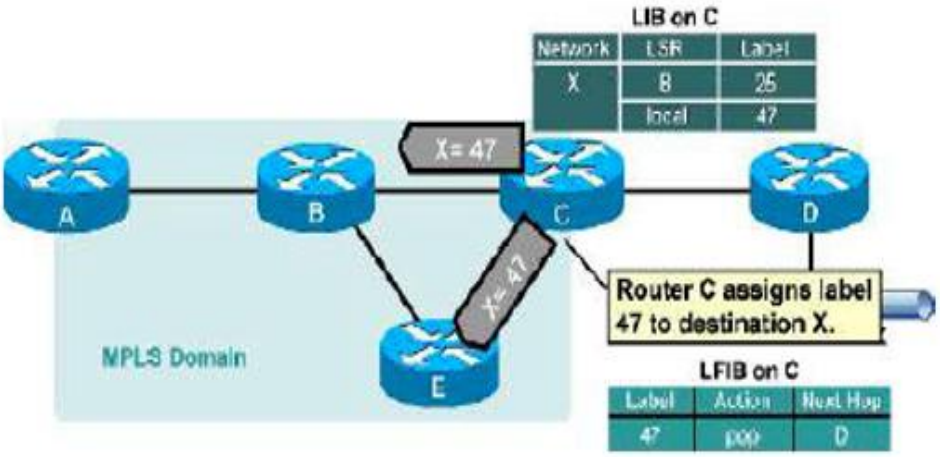

Рисунок 2.9 - Наполнение таблицы LIB

Представим, что за роутером D есть сеть X. Необходимо от этой сетки обратиться к сетке роутера A. Роутер C у нас является edge LSR (не все интерфейсы mpls), этот роутер создает локальную метку с номером 47 для сети X, после чего эту метку по протоколу LDP распространяет своим соседям: B и E (рисунок 2.11).

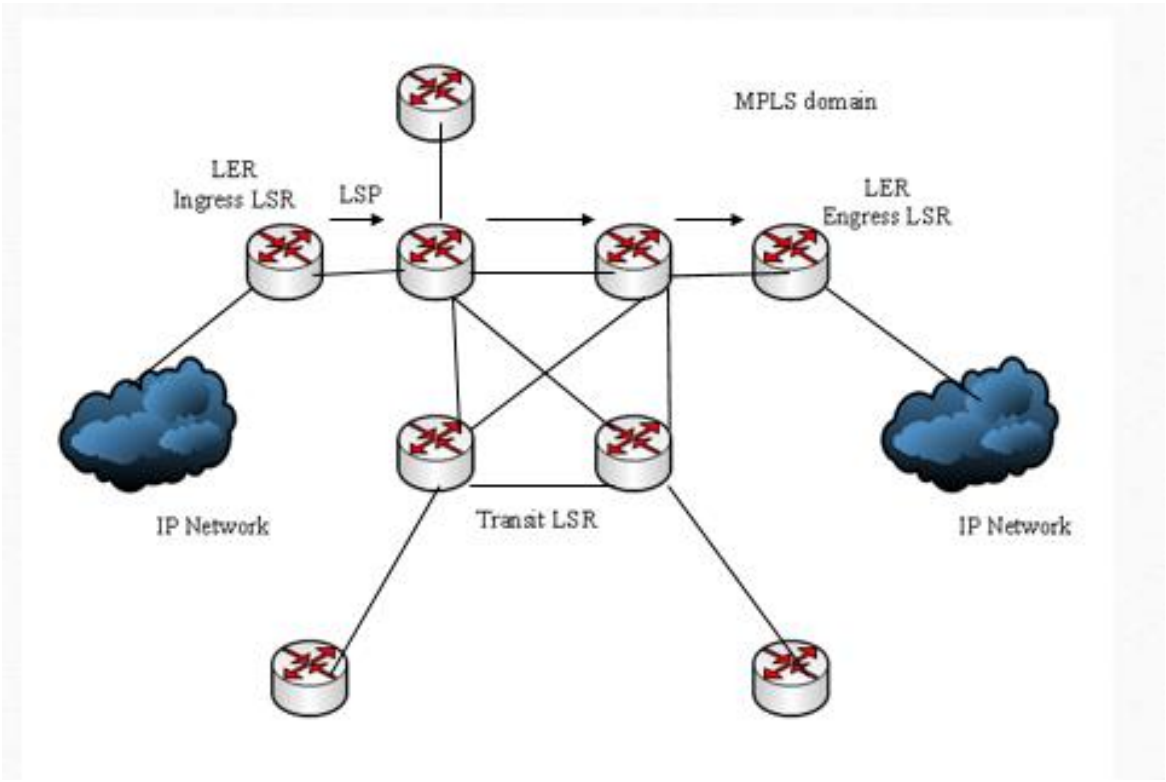

Рисунок 2.10 - Создание меток таблицы LIB

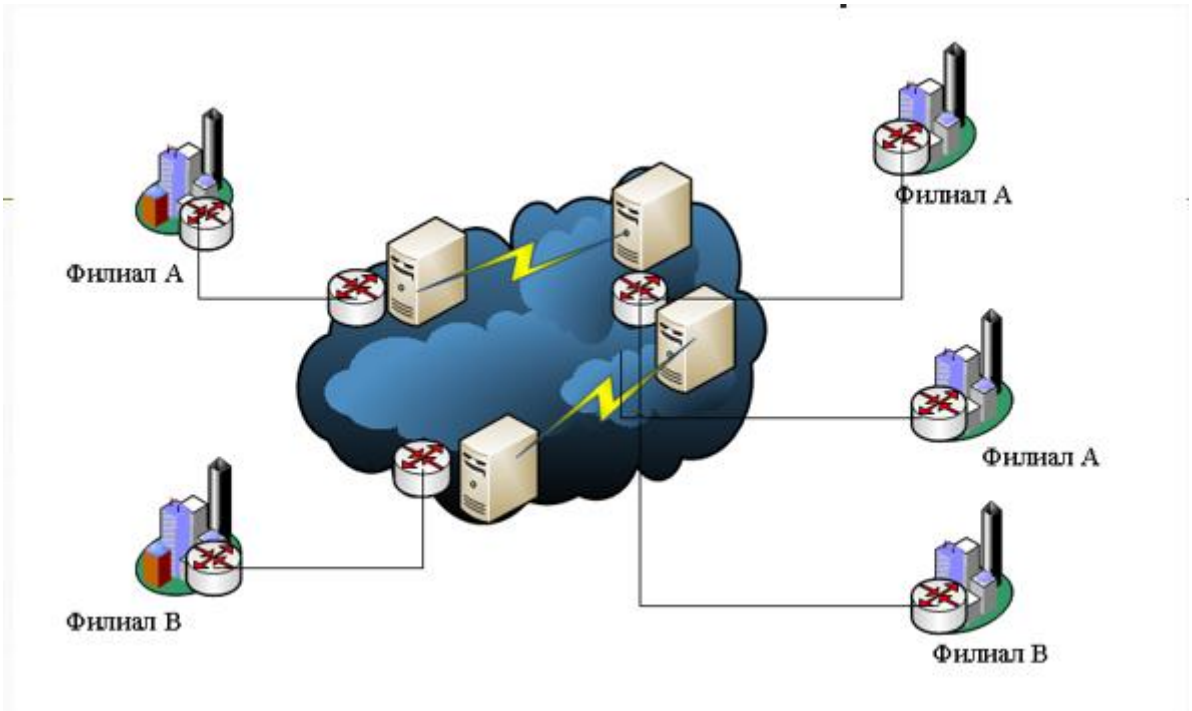

Рисунок 2.11 - Использование метки для построения IP VPN

В создает локальную метку 25, а Е — 47 и так же все это распространяется своим соседям.

Роутер А получает метку 25 от соседа В, и формирует локальную метку 12 для этого маршрута, но так как это пограничный роутер, то эта метка отбрасывается, и дальше все идет по обычному IP forwarding.

LFIB:

После того как таблица LIB заполнена, выбираются лучшие записи и помещаются в LFIB (рисунок 2.12).

Router	Label	Action	Next-hop
A	12	25	B

Router	Label	Action	Next-hop
B	25	47	C

Router	Label	Action	Next-hop
C	47	pop	D

Router	Label	Action	Next-hop
E	75	47	C

Рисунок 2.12 - Записи в LFIB

Лучшие маршруты определяются на основе IGP протокола.

FIB:

На edge роутерах, к маршруту мы должны привязать метку (рисунок 2.13).

Router	Network	Next-hop	Label
A	X	B	25

Router	Network	Next-hop	Label
B	X	C	47

Router	Network	Next-hop	Label
C	X	D	----------

Router	Network	Next-hop	Label
E	X	C	47

Рисунок 2.13 - Метки на edge роутерах

Для начала необходимо настроить базовый MPLS между всеми устройствами:

На всех роутерах прописывается конфигурация:

```
conf t
mpls ip
mpls label protocol ldp
mpls ldp router-id loopback0
mpls ldp advertise-labels
!
int s1/0
mpls ip
exit
int s1/1
mpls ip
exit
```

Так же необходимо включить mpls на интерфейсах f0/0 на роутерах p9-p10 и на интерфейсах E3/0 на роутерах PE4 и PE6.

Первое, что необходимо сделать, это включить MPLS глобально. Это делается с помощью mpls ip в режиме глобальной конфигурации.

Далее, необходимо выбрать протокол, в нашем случае мы используем протокол LDP, (cisco протокол TDP уже устарел, сейчас используется везде LDP).

Далее, необходимо следовать правилу, что пиринг лучше всего строить по лупбакам, это так же распространяется и на MPLS, поэтому надо сообщить роутеру, что router-id будет равен IP адресу лупбеку — mpls ldp router-id loopback0.

mpls ldp advertise-labels — говорит роутеру, что все интерфейсы отсылают mpls метки.

И далее на каждом интерфейсе необходимо активировать mpls дополнительно.

После того как были произведены все действия для конфигурации mpls, необходимо посмотреть на каких интерфейсах включен mpls с помощью команды show mpls interface:

```
PE-6#show mpls interfaces
Interface              IP             Tunnel   BGP Static Operational
Serial1/0              Yes (ldp)      No       No  No     Yes
Serial1/1              Yes (ldp)      No       No  No     Yes
Ethernet3/0            Yes (ldp)      No       No  No     Yes
PE-6#
```

Рисунок 2.14 - Задействованные интерфейсы

```
PE-6#show mpls interface s1/1 detail
Interface Serial1/1:
        IP labeling enabled (ldp):
          Interface config
        LSP Tunnel labeling not enabled
        BGP labeling not enabled
        MPLS operational
        MTU = 1500
PE-6#
```

Рисунок 2.15 - Можно более детально посмотреть информацию о каком-то интерфейсе

```
PE-6#show mpls ldp parameters
Protocol version: 1
Session hold time: 180 sec; keep alive interval: 60 sec
Discovery hello: holdtime: 15 sec; interval: 5 sec
Discovery targeted hello: holdtime: 90 sec; interval: 10 sec
Downstream on Demand max hop count: 255
LDP for targeted sessions
LDP initial/maximum backoff: 15/120 sec
LDP loop detection: off
PE-6#
```

Рисунок 2.16 - Параметры LDP

```
PE-6#show mpls ldp discovery
 Local LDP Identifier:
    6.6.6.6:0
    Discovery Sources:
    Interfaces:
        Serial1/0 (ldp): xmit/recv
            LDP Id: 10.10.10.10:0
        Serial1/1 (ldp): xmit/recv
            LDP Id: 8.8.8.8:0
        Ethernet3/0 (ldp): xmit/recv
            LDP Id: 4.4.4.4:0
PE-6#
```

Рисунок 2.17 – Информация о соседях mpls

Из вывода видно, что есть соседство с тремя роутерами, router-id которые равны 10.10.10.10, 8.8.8.8, 4.4.4.4. И соответственно интерфейсы, через которые доступны эти роутеры.

Можно вывести информацию более подробно, если это необходимо (рисунок 2.18).

```
PE-6#show mpls ldp discovery detail
 Local LDP Identifier:
    6.6.6.6:0
    Discovery Sources:
    Interfaces:
        Serial1/0 (ldp): xmit/recv
            Enabled: Interface config
            Hello interval: 5000 ms; Transport IP addr: 6.6.6.6
            LDP Id: 10.10.10.10:0
              Src IP addr: 191.66.60.10; Transport IP addr: 10.10.10.10
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
              Reachable via 10.10.10.10/32
              Password: not required, none, in use
        Serial1/1 (ldp): xmit/recv
            Enabled: Interface config
            Hello interval: 5000 ms; Transport IP addr: 6.6.6.6
            LDP Id: 8.8.8.8:0
              Src IP addr: 191.66.68.8; Transport IP addr: 8.8.8.8
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
              Reachable via 8.8.8.8/32
              Password: not required, none, in use
        Ethernet3/0 (ldp): xmit/recv
            Enabled: Interface config
            Hello interval: 5000 ms; Transport IP addr: 6.6.6.6
            LDP Id: 4.4.4.4:0
              Src IP addr: 191.66.46.4; Transport IP addr: 4.4.4.4
              Hold time: 15 sec; Proposed local/peer: 15/15 sec
              Reachable via 4.4.4.4/32
              Password: not required, none, in use
PE-6#
```

Рисунок 2.18 - Интерфейсы, через которые доступны роутеры

Есть практически аналог этого вывода (рисунок 2.19).

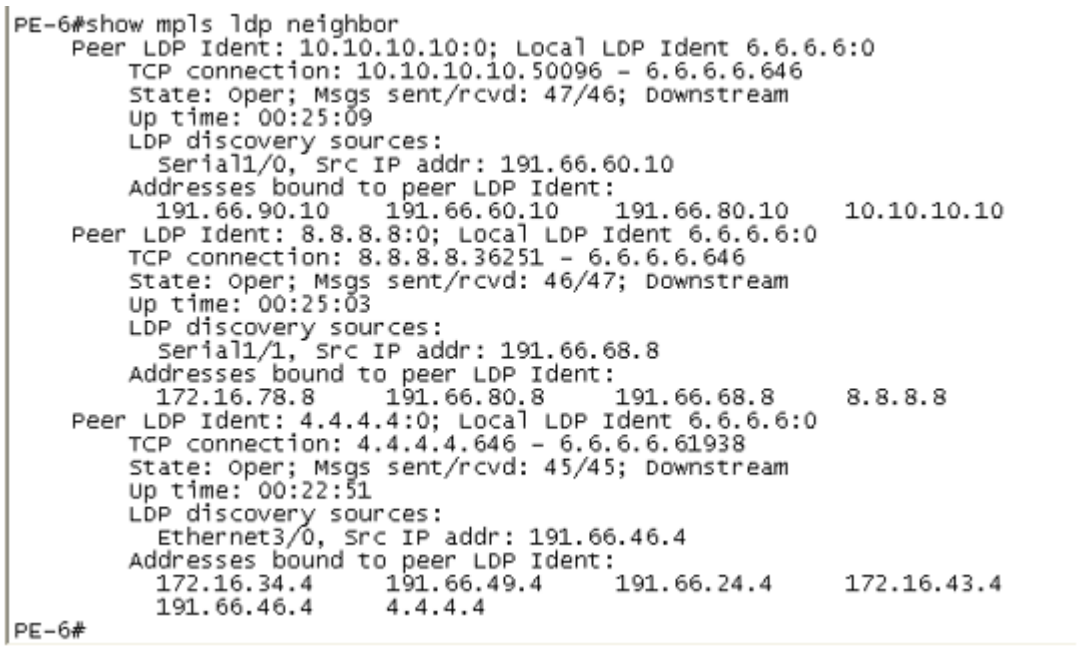

Рисунок 2.19 - Интерфейсы, через которые доступны роутеры

Просмотр базы LIB (Label Information Base) указано ниже:
PE-6#show mpls ldp bindings
lib entry: 2.2.2.2/32, rev 6
local binding: label: 18
remote binding: lsr: 10.10.10.10:0, label: 16
remote binding: lsr: 8.8.8.8:0, label: 16
remote binding: lsr: 4.4.4.4:0, label: 16
lib entry: 4.4.4.4/32, rev 4
local binding: label: 17
remote binding: lsr: 10.10.10.10:0, label: 17
remote binding: lsr: 8.8.8.8:0, label: 17
remote binding: lsr: 4.4.4.4:0, label: imp-null
lib entry: 6.6.6.6/32, rev 26
local binding: label: imp-null
remote binding: lsr: 10.10.10.10:0, label: 24
remote binding: lsr: 8.8.8.8:0, label: 18
remote binding: lsr: 4.4.4.4:0, label: 17
lib entry: 8.8.8.8/32, rev 18
local binding: label: 24
remote binding: lsr: 10.10.10.10:0, label: 25
remote binding: lsr: 8.8.8.8:0, label: imp-null
remote binding: lsr: 4.4.4.4:0, label: 18
lib entry: 9.9.9.9/32, rev 20
local binding: label: 25
remote binding: lsr: 10.10.10.10:0, label: 26
remote binding: lsr: 8.8.8.8:0, label: 19
remote binding: lsr: 4.4.4.4:0, label: 19

lib entry: 10.10.10.10/32, rev 22
local binding: label: 26
remote binding: lsr: 10.10.10.10:0, label: imp-null
remote binding: lsr: 8.8.8.8:0, label: 20
remote binding: lsr: 4.4.4.4:0, label: 20
lib entry: 172.16.34.0/24, rev 34
remote binding: lsr: 4.4.4.4:0, label: imp-null
lib entry: 172.16.43.0/24, rev 35
remote binding: lsr: 4.4.4.4:0, label: imp-null
lib entry: 172.16.56.0/24, rev 28
local binding: label: imp-null
lib entry: 172.16.78.0/24, rev 33
remote binding: lsr: 8.8.8.8:0, label: imp-null
lib entry: 191.66.24.0/24, rev 2
local binding: label: 16
remote binding: lsr: 10.10.10.10:0, label: 23
remote binding: lsr: 8.8.8.8:0, label: 21
remote binding: lsr: 4.4.4.4:0, label: imp-null
lib entry: 191.66.29.0/24, rev 14
local binding: label: 22
remote binding: lsr: 10.10.10.10:0, label: 22
remote binding: lsr: 8.8.8.8:0, label: 22
remote binding: lsr: 4.4.4.4:0, label: 21
lib entry: 191.66.46.0/24, rev 30
local binding: label: imp-null
remote binding: lsr: 10.10.10.10:0, label: 21
remote binding: lsr: 8.8.8.8:0, label: 23
remote binding: lsr: 4.4.4.4:0, label: imp-null
lib entry: 191.66.49.0/24, rev 16
local binding: label: 23
remote binding: lsr: 10.10.10.10:0, label: 20
remote binding: lsr: 8.8.8.8:0, label: 24
remote binding: lsr: 4.4.4.4:0, label: imp-null
lib entry: 191.66.60.0/24, rev 24
local binding: label: imp-null
remote binding: lsr: 10.10.10.10:0, label: imp-null
remote binding: lsr: 8.8.8.8:0, label: 25
remote binding: lsr: 4.4.4.4:0, label: 22
lib entry: 191.66.68.0/24, rev 32
local binding: label: imp-null
remote binding: lsr: 10.10.10.10:0, label: 19
remote binding: lsr: 8.8.8.8:0, label: imp-null
remote binding: lsr: 4.4.4.4:0, label: 23
lib entry: 191.66.80.0/24, rev 12

local binding: label: 21
remote binding: lsr: 10.10.10.10:0, label: imp-null
remote binding: lsr: 8.8.8.8:0, label: imp-null
remote binding: lsr: 4.4.4.4:0, label: 24
lib entry: 191.66.90.0/24, rev 8
local binding: label: 19
remote binding: lsr: 10.10.10.10:0, label: imp-null
remote binding: lsr: 8.8.8.8:0, label: 26
remote binding: lsr: 4.4.4.4:0, label: 25
lib entry: 191.66.91.0/24, rev 10
local binding: label: 20
remote binding: lsr: 10.10.10.10:0, label: 18
remote binding: lsr: 8.8.8.8:0, label: 27
remote binding: lsr: 4.4.4.4:0, label: 26
PE-6#

И базу данных LFIB:

```
PE-6#show mpls fo
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     23            191.66.24.0/24   0             Se1/0       191.66.60.10
17     17            4.4.4.4/32       0             Se1/0       191.66.60.10
18     16            2.2.2.2/32       0             Se1/0       191.66.60.10
19     Pop Label     191.66.90.0/24   0             Se1/0       191.66.60.10
20     18            191.66.91.0/24   0             Se1/0       191.66.60.10
21     Pop Label     191.66.80.0/24   0             Se1/0       191.66.60.10
22     22            191.66.29.0/24   0             Se1/0       191.66.60.10
23     20            191.66.49.0/24   0             Se1/0       191.66.60.10
24     25            8.8.8.8/32       0             Se1/0       191.66.60.10
25     26            9.9.9.9/32       0             Se1/0       191.66.60.10
26     Pop Label     10.10.10.10/32   0             Se1/0       191.66.60.10
PE-6#
```

Рисунок 2.20 - Просмотр базы LIB

Для примера можно просмотреть сеть 9-ок:

```
P-9#show mpls forwarding-table 9.9.9.9
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
None   No Label      9.9.9.9/32       0             aggr-punt
P-9#
```

Рисунок 2.21 - Сеть 9

Видно, что меток нет, т.к. тут она порождается, необходимо проверить на другом роутере.

```
P-10#show mpls forwarding-table 9.9.9.9
Local  Outgoing    Prefix           Bytes tag  Outgoing    Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
26     Pop tag     9.9.9.9/32       0          Fa0/0       191.66.90.9
P-10#
```

Рисунок 2.22 - Проверка на другом роутере

Здесь уже есть метка, но в сторону девяток ничего не посылается, то есть метка вырезается.

Посмотрим еще на PE8:

```
PE-8#show mpls forwarding-table 9.9.9.9 32
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
19     26            9.9.9.9/32       0             Se1/0       191.66.80.10
PE-8#
```

Рисунок 2.23 - Метка

Видно, что локальная метка 19, а отправлять необходимо на 26-ую.

Можно просмотреть traceroute и увидеть какие LSR проходит (рисунок 2.24).

```
PE-8#traceroute 9.9.9.9 so lo0

Type escape sequence to abort.
Tracing the route to 9.9.9.9

  1 191.66.80.10 [MPLS: Label 26 Exp 0] 116 msec 108 msec 104 msec
  2 191.66.90.9 136 msec *  132 msec
PE-8#
```

Рисунок 2.24 - LSR

Traceroute это и есть LSP.

Так как работает CEF, а он работает для MPLS всегда, можно посмотреть, что там в нем происходит (рисунок 2.25).

```
PE-8#show ip cef 9.9.9.9 detail
9.9.9.9/32, epoch 0
  local label info: global/19
  nexthop 191.66.80.10 Serial1/0 label 26
PE-8#
```

Рисунок 2 .25- Работа CEF

В итоге видно, что локальная метка 19, метка следующего хопа — 26, собственно так будет коммутироваться пакет.

3 Безопасность жизнедеятельности

Решение проблемы БЖД заключается в обеспечении нормальных и комфортных условий труда людей в их жизнедеятельности, защите человека и окружающей среды от воздействия вредных факторов, контроле нормативного уровня до приемлемого. Программное обеспечение и поддержание оптимальных, и даже хороших вещей, и минимальные сроки и условия работы человека способствуют и большей эффективности и производительности труда.

Труд и отдых, безопасность, способствующие сохранению жизни или здоровья людей за счет снижения травматизма и заболеваемости.

Вопросы безопасности, жизни вы должны иметь дело на всех этапах жизненного цикла, независимо от того, идет ли речь о разработке, эксперименте или применении, основываясь на методологии на практике.

Работа с компьютерной техникой с завистью относится к безопасному (риск смерти на одного человека в год (менее 0,0001). Значимость работы сотрудника, она также минимальна, так как уровень умственной нагрузки в данном виде деятельности обеспечивает энергозатраты 2000 г...2400 ккал в день.

Однако работник на работе с компьютерной техникой является субъектом комплекса неблагоприятных факторов, обусловленных характером процесса изготовления условий выполнения работы:

- повышенный темп работы и монотонность;
- специфика визуальной работы;
- рассеивание тепла оборудованием;
- последствия шума;
- воздействие ионизирующих и вредных газов;
- хорошие условия окружающего освещения, в помещении и на рабочем месте.

Проведен анализ условий проведения операций и мероприятий по защите от воздействия опасных производственных факторов.

3.1 Определение категории тяжести труда через интегральную бальную оценку

Условия труда – это совокупность факторов внешней производственной среды, влияющих на здоровье и работоспособность человека во время выполнения работы. Эти факторы делятся на 4 группы.

Санитарно-гигиенические факторы характеризуют производственную среду рабочей зоны (влажность, температура воздуха, освещенность, наличие шума и вибраций, электромагнитных излучений). Воздействие применяемого оборудования и технологических процессов определяет наличие этих факторов в процессе труда. Все показатели санитарно-гигиенических факторов нормированы и оцениваются количественно.

Психофизиологические факторы (тяжесть труда) обусловлены самим процессом труда. Они характеризуются физической нагрузкой, нервным напряжением, темпом работы и ее монотонностью.

Эстетические факторы (элементы) характеризуются цветовым оформлением рабочих мест и помещений, эстетизацией трудового процесса, продуктом труда, окружающей средой рабочей среды и определяющим восприятие рабочей среды и ее элементов трудящимися.

Социально-психологические факторы характеризуются сплоченностью команды, межгрупповыми отношениями в коллективе. Эти факторы определяют психологический климат в рабочей силе.

Условия труда оказывают большое влияние на здоровье персонала и его работоспособность.

Чтобы избежать негативного воздействия вредных производственных факторов, снизить производительность труда, предотвратить возникновение профессиональных заболеваний, необходимо планировать и осуществлять мероприятия по улучшению условий труда. Для этого необходимо проанализировать условия труда и определить уровень выполняемой работы.
Для оценки влияния вредных факторов на здоровье и производительность труда можно нивелировать используемые категории работ, что учитывает суммарный эффект всех факторов производственной среды.

Вследствие влияния вредных производственных факторов в трудовом процессе могут формироваться три функциональных состояния организма: нормальное, пограничное (между нормой и патологией и патологическое.

Согласно действующей классификации, условия труда можно разделить на 6 категорий, причем работа гравитационная.

Первая категория веса-к ней нужно отнести те виды работ, которые можно выполнять в идеальных условиях наружного производства на окружающую среду, а также оптимальную физическую, психическую и нервно-эмоциональную нагрузку. В этом случае объем работы соответствует физиологическим функциям человеческого организма и его возможностям.

Ко второй категории тяжести относятся вещества, в результате которых образуются уровни вредных и опасных производственных факторов, не превышающие оптимальных или предельно допустимых значений. При этом работоспособность не ухудшается, отсутствуют отклонения в состоянии здоровья, которые могут быть связаны с их профессиональной деятельностью. Возможные функциональные изменения исчезают во время проведения мероприятия.

Третья категория тяжести-нужно учитывать работу, которую предстоит выполнять в окружающей среде, когда это практически здоровые люди, опыт, реакцию, в частности, на экстремальное состояние организма. Наблюдается незначительное снижение показателей рынка труда (производительности труда). Использование альтернативных режимов работы и отдыха позволяет быстро устранить эти негативные последствия.

Четвертая категория тяжести включает в себя рабочую силу, в результате которой организм может образовать достаточно глубокое пограничное состояние, причем даже у почти здоровых особей. Большинство физиологических показателей ухудшается (не читается), особенно в конце смены или рабочего воскресенья. Отличительной особенностью ситуации, возникающей при производстве, может быть проявление.

В категорию гравитации-это работа, которая в конце смены и / или рабочей группы воскресенья создает реакцию, особенно на патологическое состояние организма Бегущего не по здоровью человека, а на то, что, как правило, исчезает на многих местах в полноценный отпуск. Однако некоторые люди меняются, и это может привести к производству оборудования и профессиональным заболеваниям.

Шестая категория — тяжести-это работа, которая четко проявляется в симптомах патологического состояния в организме человека. Эти работы должны выполняться, в частности, по опасным (критическим) требованиям задания. В то же время патологические реакции могут развиваться очень быстро, могут быть невозвратными и часто сопровождаться серьезным нарушением функций жизненно важных организмов и систем.

Характеристики микроклимата имеют и возможность изменять течение большого радиуса, при этом дело в том, что обстоятельством в жизни человека считается поддержание стабильности температуры тела за счет терморегуляции, или способности организма регулировать температуру в ответ на воздействие окружающей среды. Принцип значения микроклимата-создание оптимальных условий с целью теплообмена организма человека с окружающей средой.

Компьютерная техника считается основой важного тепловыделений того, что она способна вызывать повышение температуры и снижение относительной влажности воздуха в замкнутом пространстве. В помещениях, где перечислены компьютеры, необходимо соблюдать определенный микроклимат стандартов. При применении санитарных норм сон-245-71 определяются размеры объектов, климатические условия и создаются соответствующие условия. Эти стандарты определяются с точки зрения времени года, характера рыночного процесса и характера производства веб-сайта (см. таблицу ниже 3.1).

Объем помещения в каковых, подлежащего размещению на персонал компьютерных служб, должен быть не менее 19,5м3 / чел. с учетом максимального количества одновременных изменений. Хорошо известный Flow приток свежего воздуха к участку, где находится ваш компьютер, приведен в таблице 3.2 [1].

Таблица 3.1 - Параметры микроклимата для помещений, где установлены компьютеры

Период года	Параметр микроклимата	Величина
Холодный	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	22…24°С 40…60% до 0,1м/с
Теплый	Температура воздуха в помещении Относительная влажность Скорость движения воздуха	23…25°С 40…60% 0,1…0,2м/с

Таблица 3.2 - Нормы подачи свежего воздуха в помещения, где расположены компьютеры [1].

Характеристика помещения	Объемный расход подаваемого в помещение свежего воздуха, $м^3$ /на одного человека в час
Объем до $20м^3$ на человека $20…40м^3$ на человека	Не менее 30 Не менее 20 Естественная вентиляция

С целью предоставления удобных условий применяются как организационные методы (здравая предприятие выполнения работ в зависимости от времени и дней, смена работы и отдыха), таким образом и технические средства (вентиляция, кондиционирование воздуха, отопительная система).

Сроки и условия проведения операции оказывают непосредственное влияние и на состояние организма, и характеризуются определенной сопротивляемостью. Чтобы оценить влияние на людей внешних требований, нам необходимо определить категорию тяжести выполняемой работы.

При количественном анализе тяжести труда необходимо учитывать гигиенические требования и психофизиологические факторы производственной среды, характеризующие условия труда на рабочем месте.

К применению санитарных факторов производственной среды по ГОСТу следует отнести [2] :

- микроклимат в рабочей зоне предприятия;
- наличие и концентрация вредных веществ в различных категориях риска;
- наличие и концентрация производства пыли;
- виброакустические факторы и ультразвук;
- интенсивность теплового излучения;
- электромагнитное излучение различной частоты;
- Radiation излучение (рентгеновские лучи, гамма-лучи и А-В-излучение);
- биологический фактор.

К психосоциальным факторам риска по ГОСТу следует отнести:
- о физических, динамических и статических нагрузках;
- остановите работу и путешествуйте по карте;
- сменность, продолжительность непрерывной работы в течение дня;
- вставить в визуальные произведения;
- количество соответствующих испытательных установок;
- ритм работы, монотонность работы;
- громкость звука, и информация предоставляется перерабатываемой;
- режим работы и все остальное;
- нервно-эмоциональная нагрузка;
- Ментальное давление.

В ходе анализа учитываются факторы рабочей среды, которые специфичны для конкретной работы и отрасли. Вообще говоря, условия труда определяются суммой факторов рабочей среды, и любой показатель или фактор среды, который вы должны войти в балл, колеблется от 1 до 6, в зависимости от типа числового значения.

Категория тяжести и интенсивности операции непосредственно связана с точечной оценкой, которая определяется уравнением [3].:

$$U_r = \left[X_{max} + \frac{\sum_{i=1}^{n} X_i}{n-1} \times \frac{6 - X_{max}}{6}\right] \times 10 \quad (3.1)$$

где X_{max} - самая большая из полученных частных балльных оценок;

X_i - балльная оценка по i-му из учитываемых факторов;

n - общее число факторов без учета одного фактора X_{max};

N - общее количество факторов.

Зависимость категории тяжести от интегральной балльной оценки приведена в таблице 3.3 [3].

Таблица 3.3 - Категории тяжести труда

Категория тяжести труда	1	2	3	4	5	6
Интегральная оценка элементов условий труда, U_T, баллы	до 18	18,1- 33	33,1- 45	45,1- 53	53,1- 59	59,1- 60

Если вредный фактор оказывает воздействие не в течение всей рабочей смены, то оценка факторов и показателей условий труда должна быть определена в зависимости от времени их воздействия на работника [4] :

$$X_{i\text{факт}} = X_i \frac{t}{t_{см}} \quad (3.2)$$

где X_i - оценка i-го элемента условий труда в баллах;

t- фактическая длительность действия фактора, мин.;

$t_{см}$- продолжительность смены, мин.

Повышение тяжести труда будет влиять на работоспособность человека. Снижение работоспособности непосредственно связано с состоянием утомления, которое количественно можно оценить при помощи показателя утомления, выраженного в условных единицах. Зависимость между интегральным показателем тяжести труда и степенью утомлением можно выразить уравнением: [4]

$$У = \frac{U_T - 15,6}{0,64} \quad (3.3)$$

где У - показатель утомления в условных единицах;

15,6 и 0,64 - коэффициенты регрессии;

U_T - интегральный показатель категории тяжести труда в баллах.

Если знать степень утомления, то можно определить уровень работоспособности по формуле:

$$R = 100 – У \quad (3.4)$$

где R - уровень работоспособности в относительных единицах.

По значениям работоспособности, которые определили до и после проведения мероприятий по улучшению условий труда, теперь можно рассчитать изменение производительности труда (прирост производительности) по формуле:

$$П_{пт} = \left[\frac{R_2}{R_1} - 1\right] \times 100 \times 0,2 \quad (3.5)$$

где $П_{пт}$ - прирост производительности труда;

R_2 и R_1 - работоспособность в условных единицах до и после проведения мероприятий по улучшению и оздоровлению условий труда;

0,2 - поправочный коэффициент, который отражает зависимость между увеличением работоспособности и ростом производительности труда.

Тяжесть и напряженность труда оказывает влияние на рост производственного травматизма. Так как интегральная балльная оценка дает возможность определить категорию тяжести труда, то величину производственного травматизма можно рассчитать по формуле[5]:

$$К = \frac{1}{1,3 - 0,0185 \cdot U_T} \quad (3.6)$$

где К - рост производственного травматизма, количество раз;

U_T - интегральный показатель категории тяжести труда в баллах.

На рабочих местах необходимо предусмотреть создание благоприятной производственной среды и формирование условий труда, относящихся к первой категории тяжести труда (оптимальные). Если оборудование имеет малую травм опасность и большую производительность, то величину травматизма можно принять равной единице, и в данном случае, интегральный показатель тяжести труда будет равен [5]:

$$U_T = (1,3 – 1,0) / 0,0185 = 16,2 \quad (3.7)$$

что характеризует наилучшую травм безопасность данного рабочего места.

3.2 Определение категории тяжести и напряженности труда специалиста ПЭВМ

Таблица 3.4 - Исходные данные для выполнения расчета

Профессия	Фактор рабочей среды и условия труда	Значение показателя до модернизации	Значение показателя после модернизации	Продол. времени действия
Специалист	Температура воздуха на РМ в теплый период года, C^0	33	20	480
	Превышение допустимого уровня звука, дБа	90	70	480/420
	РМ стационарное, поза свободная	-	-	480
	Масса перемещаемых грузов	до 5 кг	до 2 кг	480
	Работа в утреннюю смену	-	-	-
	Продолжительность непрерывной работы в течение суток, часов	8	6	480
	Длительность сосредоточенного наблюдения, % от продолжительности рабочей смены	80	60	480/240
	Обоснованный режим труда и отдыха с применением функциональной музыки и гимнас	-	-	-
	Нервно-эмоциональная нагрузка возникает в результате простых действий по индивидуальному плану	-	-	-

Таким образом, в результате мероприятий по безопасности и охране труда была произведена модернизация факторов рабочей среды и условия труда. А именно: замена устаревшего оборудования, разделение рабочего места специалиста, установление кондиционера, сокращение продолжительности непрерывной работы в течение суток и длительность и сосредоточенного наблюдения. Также изменились показатели факторов рабочей среды и условий труда.

По исходным данным и таблицам выставляем баллы каждому фактору рабочей среды и показателю до и после проведения мероприятий по оздоровлению условий труда. При оценке необходимо корректировать

значение балла в зависимости от времени воздействия. Результаты оценки представляем в виде таблицы (таблица 3.5).

Таблица 3.5 - Балльная оценка факторов рабочей среды и условий труда [6]

Фактор рабочей среды и условия труда	Значение показателя	Оценка факторов в баллах	
		До проведения мероприятий	После проведения мероприятий
Температура воздуха на РМ в холодный период года, C^0	33/20	5	1
Превышение допустимого уровня звука, дБа	90/70	4	2
РМ стационарное, поза свободная, масса перемещаемых грузов	5/2	2	1
Работа в утреннюю смену. Продолжительность непрерывной работы в течение суток, часов	8/6	1	1
Длительность сосредоточенного наблюдения, % от продолжитель-ности рабочей смены	80/60	3	2
Обоснованный режим труда и отдыха с применением функциональной музыки и гимнастики		2	1
Нервно-эмоциональная нагрузка возникает в результате простых действий по индивидуальному плану		1	1

*В графе "Значение показателя" в числителе указаны значения до проведения мероприятий, а в знаменателе - после.

После оценки в баллах факторов и показателей необходимо рассчитать интегральную оценку тяжести труда до и после проведения мероприятий по формуле (3.1):

а) до проведения мероприятий по улучшению условий труда:

$$U_1 = \left[5 + \frac{5+4+2+1+3+2+1}{6} \times \frac{6-5}{6}\right] \times 3 = 55{,}1$$

из таблицы 3.3 определяем, что данные условия труда относятся к пятой категории тяжести труда, значит у работника формируется достаточно устойчивое патологическое состояние, которое характеризуется замедлением реакций;

б) после проведения мероприятий по улучшению условий труда.

Так как после проведения мероприятий изменилось время воздействия факторов рабочей среды и условий труда, необходимо пересчитать оценку факторов.

Принимаем продолжительность смены равной 480 мин.

В нашем случае после проведения мероприятий изменилось время воздействия шумов (фиксировалось превышение ПДУ шума), поэтому бальную оценку необходимо провести с учетом данного изменения по формуле 3.2:

$$X_{кор\ 1} = 2 \cdot \frac{420}{480} = 1{,}75\ ,$$

и при изменении продолжительности нервно-эмоциональных нагрузок

$$X_{кор\ 2} = 2 \cdot \frac{240}{480} = 1\ .$$

Интегральная балльная оценка по формуле 3.1 после проведения мероприятий с учетом коррекции будет равна:

$$U_2 = \left[2 + \frac{1 + 1{,}75 + 1 + 1 + 2 + 1 + 1}{6} \times \frac{6 - 2}{6}\right] \times 3 = 30{,}5$$

из таблицы 3.3 определяем, что данные условия труда относятся к третьей категории тяжести труда. В таких условиях возникают реакции, характерные начальной стадии пограничного состояния организма.

Прогноз изменения травматизма после проведения мероприятий по улучшению условий труда выполняем следующим образом. Рост травматизма для пятой и третьей категории тяжести оцениваем по формуле (3.6).

Определим рост травматизма до проведения мероприятий по улучшению условий труда (формула 3.3):

$$Y_1 = \frac{1}{1{,}3 - 0{,}0185 \times 55{,}1} = 3{,}33\ ,$$

После проведения мероприятий (изменение температуры воздуха рабочей среды, уменьшение уровня шума и времени воздействия на оператора и т.д.) категория тяжести труда снизится до третьей (U2=38,3), что будет соответствовать росту травматизма в 1,69 раза по сравнению с рациональными условиями труда:

$$Y_2 = \frac{1}{1{,}3 - 0{,}0185 \times 30{,}5} = 1{,}4\ ,$$

При проведении мероприятий по улучшению условий труда категория тяжести изменилась с пятой до третьей. Как отмечалось выше тяжесть труда негативно влияет на степень утомления, а значит и работоспособность человека.

Для исследования динамики изменения работоспособности и производительности необходимо рассчитать значения показателей утомления и работоспособности:

а) до проведения комплекса мероприятий:

- показатель утомления по формуле (3.3):

$$У_1 = \frac{55,1 - 15,6}{0,64} = 62 ,$$

- уровень работоспособности по формуле (3.4):

$$R_1 = 30\text{-}62 = 83 ,$$

б) после проведения комплекса мероприятий:

- показатель утомления:

$$У_2 = \frac{30,5 - 15,6}{0,64} = 23 ,$$

- уровень работоспособности:

$$R_2 = 30 - 23 = 77.$$

5. Изменение производительности труда (прирост производительности труда) за счет изменения работоспособности по формуле 3.5 составит:

$$П_{nm} = \left[\frac{R_2}{R_1} - 1\right] \times 30 \times 0,2 = \left[\frac{77}{38} - 1\right] \times 30 \times 0,2 = 20,5 .$$

В помещении работают несколько источников шума, имеющие одинаковый уровень звуковой мощности. Источники расположены на полу (Ф=1). Источники шума находятся на расстоянии r от расчетной точки, которая расположена на высоте 1,5 м от пола. Определить октавные уровни звукового давления в расчетной точке. Привести схемы расположения расчетных точек и источников шума.

Данные расчета сравнить с нормируемыми уровнями звукового давления. В случае превышения уровня определить требуемое снижение звукового давления и рекомендовать меры защиты персонала от действия шума.

3.3 Определение расчета кратности воздухообмена

Частота воздухообмена-применение санитарного состояния замкнутой воздушной массы. При таком расположении все зависит от безопасности и комфорта людей. Допустимые значения определяются государством в строительных нормах и правилах (СНиП), сводах правил, а также (СП), санитарных правилах и стандартах (СанПиН) и ГОСТах. В большинстве соглашений об обмене указывается, сколько раз в течение одного часа, а также заменялся для новых.

Существует 2 типа изменений: естественные или искусственные. Естественный способ разделения в движении газовых потоков, из-за разницы в давлении. Из областей с большим давлением — в области с меньшим. Искусственная вентиляция предполагает работу вентиляторов, кондиционеров и других электроприборов.

Формула кратности воздухообмена выглядит так [7]:

$$N = Q / V \quad (3.6)$$

где: N или n — кратность (раз в час);

Q - нужное количество свежего воздуха в час, м³/ч;

V - объем помещения, м³; если у комнаты сложная форма, объем нужно определять вместе со специалистами.

Естественное замещение воздуха ограничивается 3-4-кратным показателем, поэтому его движение иногда приходится усиливать механической вентиляцией.

Вентиляционные системы работают по 2 схемам: вытесняют старый воздух новым или перемешивают обе эти массы.

Для систем, работающих только на удаление воздуха, основная формула кратности выглядит следующим образом: [7]

$$N = V \text{ у. в.} / V \text{ пом}, \quad (3.7)$$

где: V у. в. — объем удаляемого воздуха, м³/ч;

V пом — объем помещения, м³.

В удаляемый объем следует включать тепловые выделения и летучие вредные вещества.

Для приточной и вытяжной вентиляции рассчитывают также отдельные показатели кратности.

К примеру, для приточной системы его определяют так [7]:

$$N \text{ пр} = L \text{ пр} / V \text{ пом}, \quad (3.8)$$

где: L пр — производительность приточной системы, м³/ч;

V пом — объем помещения, м³.

На одного сотрудника следует отводить 60 м³/ч, а на временного посетителя — 20 м³/ч. Удельная кратность выступает как информативный показатель при условии, что размеры помещения приближаются к стандартным.

В офисах и административных учреждениях требуется больше свежего воздуха, чем в индивидуальном жилье. Причина этому — большое количество офисной техники, напряженная умственная деятельность и стандарты обслуживания клиентов.

Новый воздух должен эффективно удалять испарения. Стоит уделить внимание увлажнению и очистке воздуха, его охлаждению или прогреву перед подачей в помещения.

В рабочей комнате на 1 сотрудника нужно не меньше 20 м³/ч. В конференц-залах столько же отводят на каждого посетителя. Интенсивный воздухообмен следует обеспечивать в умывальных и санитарных комнатах — до 15 обновлений воздуха в час.

Возьмем для примера помещение высотой 3,5 м и площадью 60 м², где работает 15 человек. Считаем, что воздух загрязняется только от роста концентрации углекислого газа из-за дыхания.

Сначала находим объем помещения: V = 3,5 м × 60 м² = 23 м³.

Учитываем, что 1 среднестатистический человек выделяет 22,6 л углекислого газа в час [8].

Получаем, что вредные выделения можно рассчитать формулой

В = 22,6 × n, где n соответствует количеству людей в помещении.

В = 22,6 л/ч × 15 = 339 л/ч

Для помещений максимально допустимая концентрация углекислого газа равняется 1/300, или же 0,1 %. Переведем это в 1 л/м³. В чистом воздухе углекислого газа есть около 0,035 %. Переводим в 0,35 л/м³.

Рассчитаем по формуле 3.6, сколько свежего воздуха понадобится для всех 15 человек:

Q = 339 л/ч : 1 л/м³ – 0,35 л/м³ = 339 л/ч : 0,65 л/м³ = 521,5 м³/ч. Кубические метры в данном случае перешли в числитель, а часы — напротив, в знаменатель.

Определяем кратность воздухообмена (формула 3.7):

N = 521,5 м³/ч : 23 м³ = 2,48 раз в час. Выходит, при сменяемости воздуха на уровне 2,48 раз в час концентрация углекислого газа останется в пределах нормы.

Найдем теперь удельную кратность воздухозамещения на 1 человека и на 1 м². Объем помещения при этом должен быть не меньше 23 м³, а высота потолка — от 3,5 м.

521,5 м³/ч : 15 чел. = 34,7 м³/ч на 1 человека

521,5 м³/ч : 60 м² = 8,7 м³/ч на 1 м² площади

Таким образом, в помещении удельная кратность воздухозамещения на 1 человека 34,7 м³/ч, при том, что в рабочей комнате на 1 сотрудника необходимо не меньше 20 м³/ч.

Вывод

В этой главе будут проанализированы оптимальные условия эксплуатации для разработки программного обеспечения, а также необходимые меры безопасности и охраны, которые могут быть найдены.

При анализе тяжести выполняемой работы, выполняемой работы, специалист рассчитывал интегральный числовой балл. Результат расчета, определенный графиком и условиями работы специалиста, так как они относятся к весовой категории, оказывает негативное влияние на работоспособность и состояние здоровья. Необходимо было ввести в действие меры по улучшению условий труда: сокращение продолжительности воздействия шума и нервно-эмоциональной нагрузки. После введения занятий гравитационного класса работа увеличивается с повышением пятого до второго уровня. Однако норма прибыли увеличилась с 38 в относительных единицах на рисунке 77, производительность рабочей силы увеличилась на 20,5%.

4 Анализ и оценка рисков

Целью анализа рисков, связанных с эксплуатацией информационных систем, является оценка угроз (т.е. условий и факторов, которые могут стать причиной нарушения целостности системы, ее конфиденциальности, а также облегчить несанкционированный доступ к ней) и уязвимостей (слабых мест в защите, которые делают возможной реализацию угрозы), а также определение комплекса контрмер, обеспечивающего достаточный уровень защищенности ИС. При оценивании рисков учитываются многие факторы: ценность ресурсов, значимость угроз, уязвимостей, эффективность имеющихся и планируемых средств защиты и многое другое.

Процесс управления направлен на определение событий, которые могут оказать влияние на организацию, и на управление связанным с этими событиями риском. При этом обеспечивается контроль над допустимым уровнем риска при разумной гарантии достижения целей организации. Управление рисками организации представляет собой непрерывный процесс, охватывающий всю организацию, осуществляется сотрудниками на всех уровнях организации (советом директоров, менеджерами и другими сотрудниками), используется при разработке и формировании стратегии, применяется во всей организации, на каждом ее уровне и в каждом подразделении и включает анализ портфеля рисков на уровне организации.

К мерам по управлению ИТ-рисками относятся: разработка нормативных документов; обеспечение физической безопасности и безопасности ИС; разграничение доступа к ресурсам компании; контроль состояния корпоративной ИС. Во-первых, определяется объект защиты — проводится инвентаризация информационных активов, оценивается их критичность для бизнес-процессов компании. Во-вторых, решается, от чего осуществляется защита. Для этого анализируются присущие системе уязвимости, определяется степень их критичности — вероятность того, что они могут быть реализованы.

Активы, рассмотренные в данной работе:

- программно-аппаратный комплекс ФПСУ;
- ФПСУ-IP клиент;
- маршрутизатор;
- коммутатор;
- ИС Банка (терминальные сервера).

Таблица 4.1 – Активы

№	Код актива	Наименование	Кол-во	Ответственный	Ценность	Приоритет	Стоимость

Продолжение таблицы 4.1

1	FP	Программно-аппаратный комплекс ФПСУ	1	Администратор системы	4	3	20000000 тг.
2	FP-C	ФПСУ-IP клиент	1	Администратор системы	3	4	1898000тг.
3	RO	Маршрутизатор	5	Сетевой администратор	2	5	3000000 тг.
4	SW	коммутатор	3	Сетевой администратор	1	6	1500000 тг.
5	IS	ИС Банка (терминальные сервера)	30	Бизнес-владелец ИС	5	1	600000000 тг.

Основой мер защит банковской сети является Программно-аппаратный комплекс ФПСУ:

1. программно-аппаратный комплекс "ФПСУ-IP" является средством комплексного решения задач по защите информационных и телекоммуникационных систем Банка от несанкционированного доступа (НСД) и предназначен для организации управления доступом к информационным ресурсам сетей передачи данных и обеспечения целостности, достоверности и конфиденциальности сетевых соединений.
2. используется в Банке для защиты каналов передачи данных между ЦО Банка, его филиалами, УДО и устройствами самообслуживания, агентской сетью, разработчиков и ЦА СБРФ.
3. используется для идентификации и аутентификации "ФПСУ-IP/Клиентов", удалённых "ФПСУ-IP" и удалённых администраторов методами, устойчивыми к активному перехвату информации в сети;
4. дает возможность для организации туннелированной передачи данных с пакетным шифрованием;
5. используется для защиты каналов управления и мониторинга пограничными маршрутизаторами из защищённых областей;
6. позволяет реализовать контроль и управление потоками информации, а также их коммутацию из одной локальной сети в другую, что обеспечивает разграничение доступа и защиту сегментов локальной вычислительной сети от атак злоумышленников;
7. для повышения надёжности и обеспечения бесперебойной работы защищаемых подсетей в ситуации аппаратных отказов, "ФПСУ-IP" может быть задействован в режиме "горячего" резервирования, позволяющую вместо одного "ФПСУ-IP" использовать пару "ФПСУ-IP", один из которых выполняет все функциональные операции, а второй находится в ожидании, готовый принять управление на себя в случае неполадок на основном "ФПСУ-IP".

8. обеспечивает фильтрацию сетевых пакетов в соответствии с типами отправителя и получателя (абонент, маршрутизатор, удалённый "ФПСУ-IP", клиент, удалённый администратор) по задаваемым администратором правилам, IP-адресам отправителя и получателя

9. обеспечивает защиту от несанкционированного доступа при работе удалённого администратора методами, устойчивыми к активному перехвату информации в сети посредством двусторонней аутентификации.

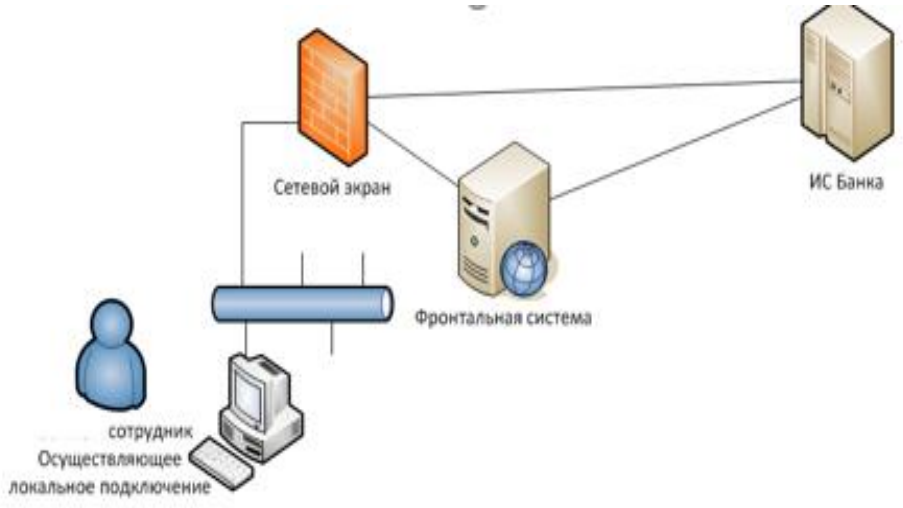

Рисунок 4.1 - Сеть банка до применения мер

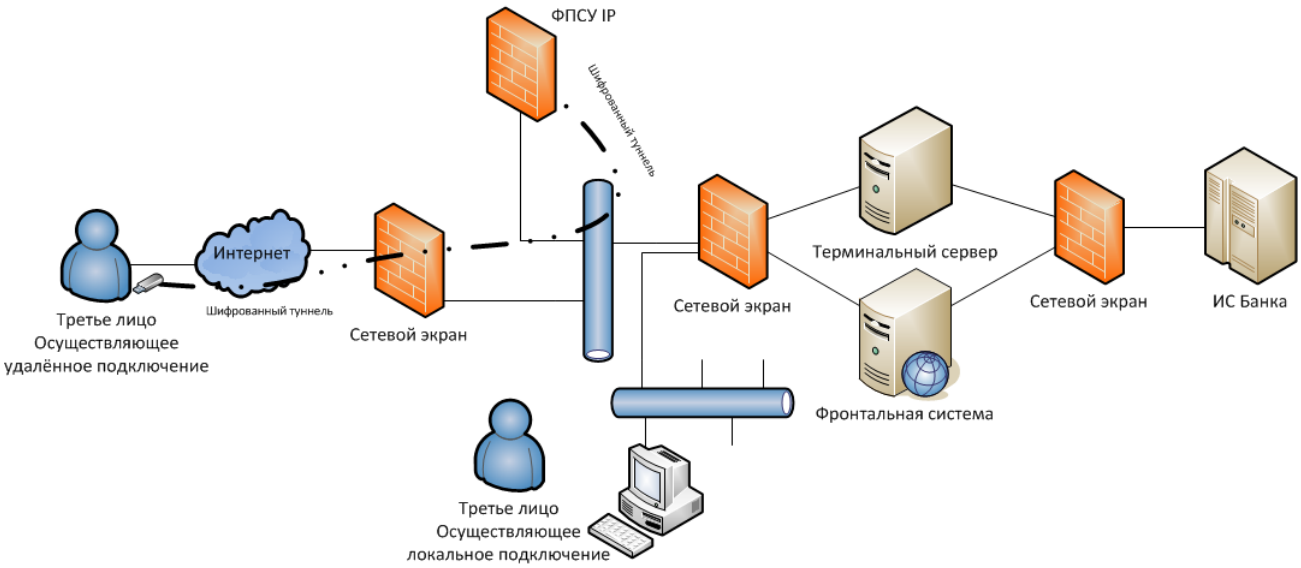

Рисунок 4.2 - Сеть банка после применения мер

4.1 Расчетная часть

Таблица 4.2 - Шкала вероятности возникновения риска

0 - очень низкий	раз в несколько лет
1 - низкий	один раз в 3 года
2 - средний	несколько раз в год
3 - высокий	один раз в месяц
4 - очень высокий	несколько раз в месяц

При расчете рисков по двум параметрам таблица использована, чтобы связать факторы последствий (ценность активов) с вероятностью возникновения угрозы. Первый шаг состоит в оценивании последствий по заранее определенной шкале, от 1 до 5, для каждого находящегося под угрозой актива. Второй шаг состоит в оценивании вероятности возникновения угрозы по заранее определенной школе (от 1 до 4). Третий шаг состоит в вычислении меры риска путем умножения ценности актива на вероятности возникновения угрозы.

Таблица 4.3 - Оценка рисков по двум параметрам

№	Угрозы	Уязвимости	Максимальный уровень риска	Меры по обработке риска	Остаточный уровень риска	Дата	Комментарий, ресурсы, ответственный
Актив: Программно-аппаратный комплекс ФПСУ							
1	НСД	Доступ к компьютеру лиц, не имеющих на это право	8	Двухфакторная аутентификация, доступ к серверу через систему мониторинга CYBER	4	31.12.2020	Сетевой Администратор
2	Сетевые атаки	Переполнение буфера (Buffer Overflow), Форматирование строки (Format String), Целочисленное переполнение (Integer Overflows), LDAP внедрение (LDAP Injection), Mail внедрение (Mail Command Injection), Нулевой байт (Null Byte Injection), Выполнение команд ОС (OS Commanding), Исполнение внешнего файла (RFI, Remote File	8	Backup системы, фильтрация трафика	4	31.12.2020	Сетевой Администратор

		Inclusion), Внедрение SSI (SSI Injection)					

Продолжение таблицы 4.3

3	Сбои и отказы работы систем	Со стороны партнера банка могут быть установлены специализированные программы по выводу из строя сервера	8	Прописать все условия по безопасности в политике о неразглашении конфиденциальности, предоставить гарантийное письмо, подписание с компанией политики о кибербезопасности	4	31.12.2020	Сетевой Администратор
Актив: Маршрутизатор							

4	Перехват трафика	Совершение несанкционированного мониторинга, IP-спуфинг.	8	В access-list заносятся записи, запрещающие доступ к PE по telnet из CE	4	31.12.2020	Сетевой Администратор
5	Перехват управления	Совершение Ddos атаки, в целях вывода из строя оборудования	8	Ограничения общего количество маршрутов, которые могут быть приняты BGP во время одной сессии	4	31.12.2020	Сетевой Администратор
6	Перехват управления	Доступ к паролям сети и личному кабинету маршрутизатора	6	Использование аутентификации в протоколах маршрутизации. Ограничения общего количества маршрутов в VRF	3	31.12.2020	Сетевой Администратор

Продолжение таблицы 4.3

Актив: ФПСУ-IP клиент							
7	Ошибки в программном обеспечении	Отказ в обслуживании, Злоупотребление SOAP	9	Backup системы	6	31.12.2020	Администратор

8	Подмена содержания (атаки на клиентов)	Content Spoofing, Cross-Site Scripting URL Redirector Abuse, Cross-Site Request Forgery), HTTP Response Splitting, (HTTP Response Smuggling,Routing Detour,HTTP Request Splitting,HTTP Request Smuggling).	6	Установка ForcePoint, ПО Kaspersky Antivirus	3	31.12.2020	Администратор
9	Кража ФПСУ ключа	Получение конфиденциальной информации, которая может быть использована недобросовестными конкурентами или преступниками для получения прибыли.	9	Установка пароля для каждого ключа индивидуально, подписать акт приема-передаче, в случае утери ключа необходимо обратиться к администратору для деактивации ФПСУ ключа	6	31.12.2020	Администратор

Продолжение таблицы 4.3

Актив: Коммутатор							
3	Перехват трафика	Совершение несанкцианированного мониторинга	8	В access-list заносятся записи, запрещающие доступ к PE по telnet из CE	4	31.12.2020	Сетевой Администратор
11	Сбой в работе	Совершение Ddos атаки, в целях вывода из строя оборудования	6	Ограничения общего количество маршрутов, которые могут быть приняты BGP во время одной сессии	3	31.12.2020	Сетевой Администратор
12	Перехват управления	Недостаточная аутентификация при доступе к ресурсам	6	Использование аутентификации в протоколах маршрутизации. Ограничения общего количества маршрутов в VRF	3	31.12.2020	Сетевой Администратор
Актив: ИС Банка (терминальные сервера)							

13	Сетевые атаки	Внедрение SQL , XPath, XML, XQuery ,XXE	3	Установка ForcePoint, ПО Kaspersky Antivirus, Использование VPN Амикон	5	31.12.2020	Бизнес-владелец

Продолжение таблицы 4.3

14	Вывод из строя	Отключение важных процессов, связанных с функционированием ИС Банка, приостановка и изменение служб и сервисов на боевых серверах ИС	3	Регулярное резервное копирование серверов	5	31.12.2020	Бизнес-владелец
15	НСД	Доступ к компьютеру лиц, не имеющих на это право	12	Двухфакторная аутентификация, доступ к серверу через систему мониторинга CYBER	6	31.12.2020	Бизнес-владелец

4.2 Анализ рисков с инструментом CORAS

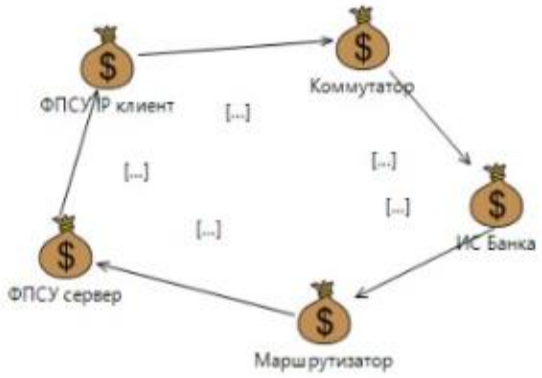

Рисунок 4.4- Активы

На рисунке 4.4 изображены защищаемые активы. Данные активы были выбраны в связи с разработкой защищенной сети банка. Акцент делается на активы ИС банка и программно-аппаратный комплекс ФПСУ IP, так как при удаленном подключении к ИС банка по VPN туннелю используется ФПСУ IP.

На рисунке 4.5 представлена диаграмма модели угроз. На диаграмме указаны: источники угроз, уязвимости, этапы реализации угроз, инциденты и активы, которые понесли ущерб из-за данных инцидентов. К примеру, источник угроз Администратор, который из-за недостаточной компетентности некорректно выдал права и роли в ИС Банка, стал причиной доступа к конфиденциальной информации в системах лиц, которым данные права не полагаются, что приводит к хищению или удалению информации.

На рисунке 4.6 изображены угрозы с учетом вероятности возникновения инцидента. На рисунке также изображены источники угроз, уязвимости, инциденты и активы.

На рисунке 4.7 представлена диаграмма рисков с характеристиками влияния угроз. К примеру, если нарушитель, используя незащищенную сеть, будет иметь доступ в сеть банка, это очень сильно повлияет на сервера и ИС Банка.

На рисунке 4.8 представлена диаграмма модели угроз с учетом защитных мер. В диаграмме добавлены защитные меры для уменьшения рисков, которые приведены в таблице 4.3. К примеру, для уязвимости НСД применена мера “Двухфакторная аутентификация и доступ к серверам через систему мониторинга”, которая значительно снижает риски.

На рисунке 4.9 представлена диаграмма недопустимых рисков.

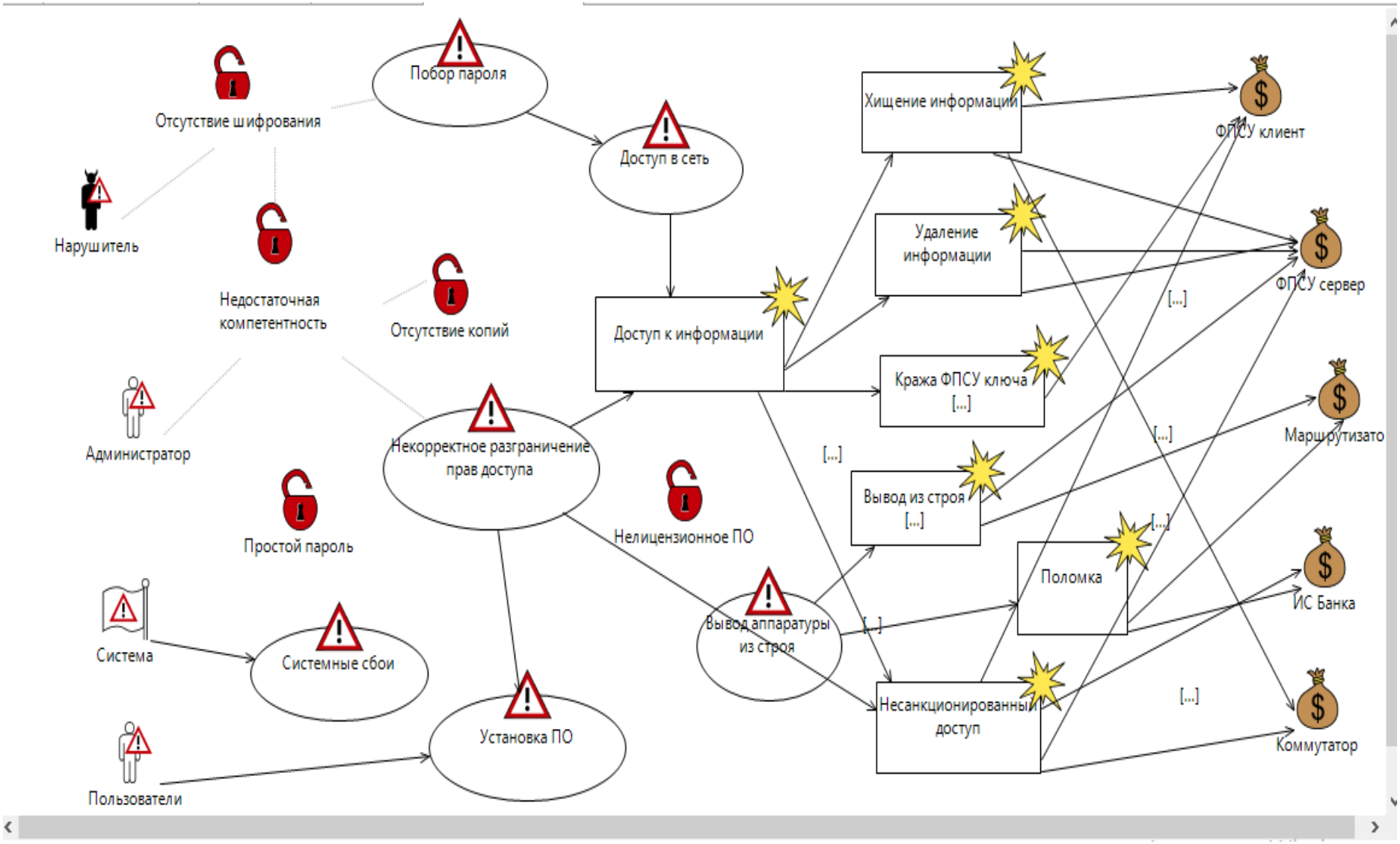

Рисунок 4.5 – Диаграмма угроз

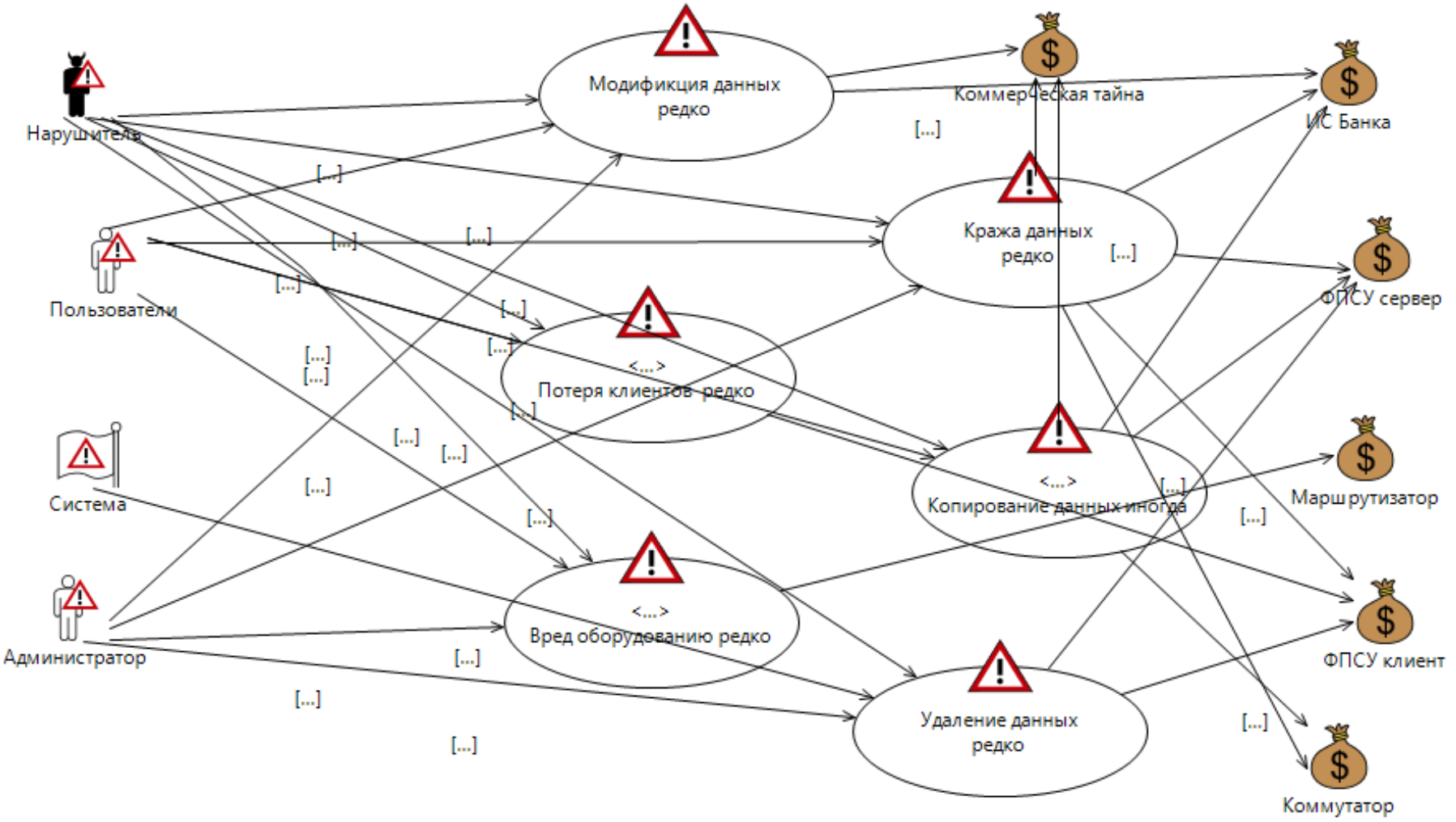

Рисунок 4.6 – Диаграмма угроз с учетом вероятности возникновения инцидента

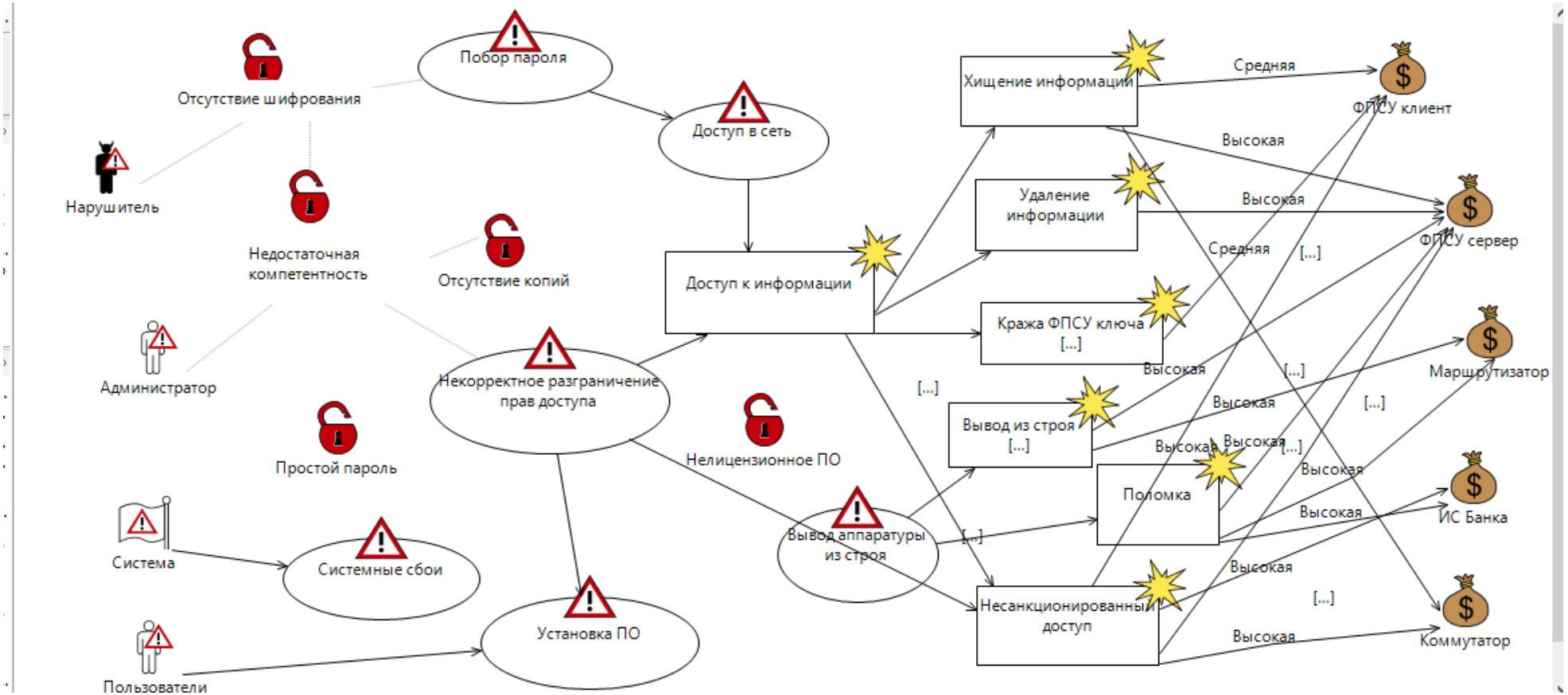

Рисунок 4.7 – Диаграмма угроз с вероятностными характеристиками

Также необходимо построить диаграмму противодействий для недопустимых рисков. На диаграмме угроз для каждой уязвимости соответствует противодействие

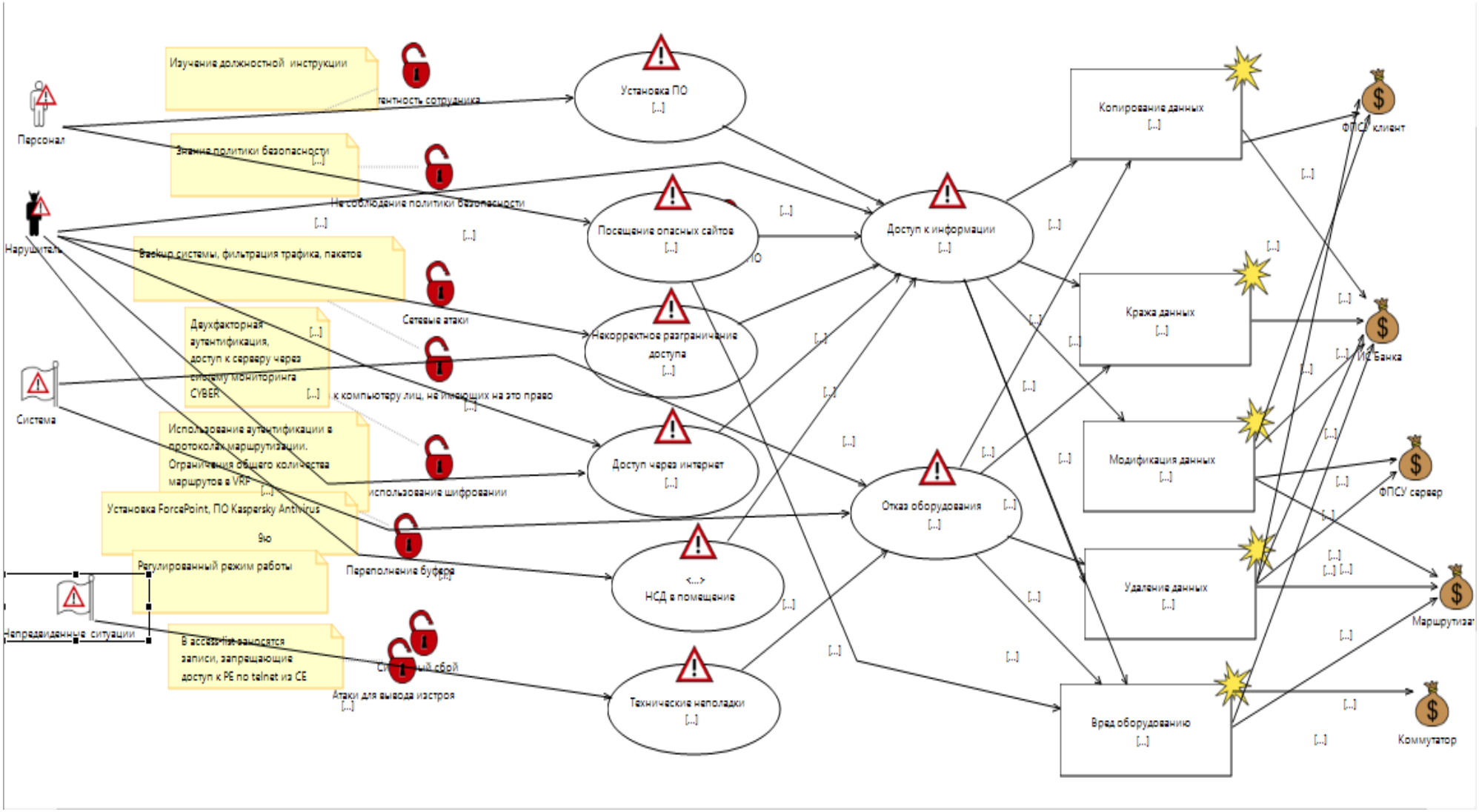

Рисунок 4.8 – Диаграмма угроз с элементами СЗИ

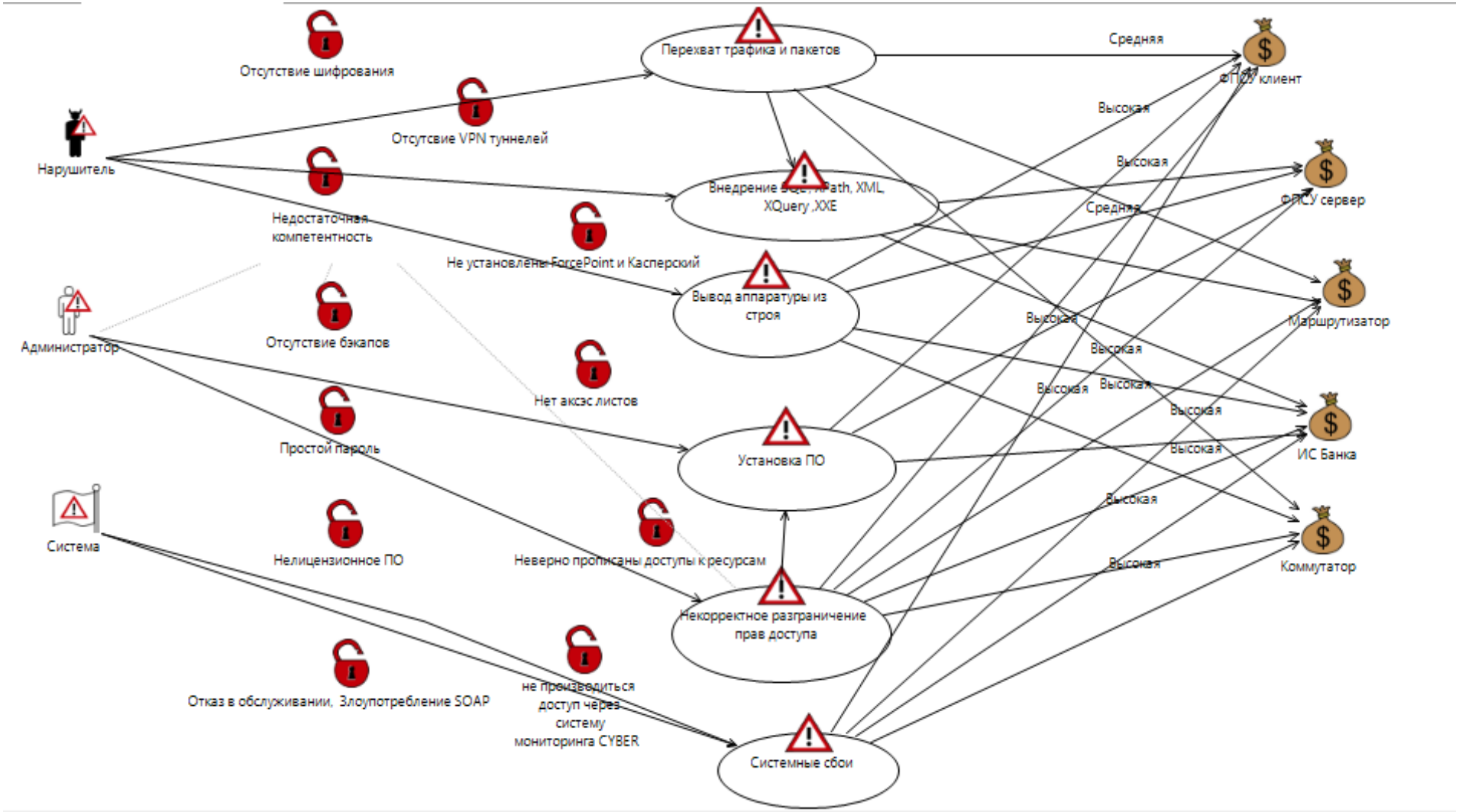

Рисунок 4.9 - Диаграмма неприемлемых рисков

Вывод

В данном разделе дипломного проекте были произведены расчеты рисков с целью выявления уязвимостей информационной системы и их устранения. Подсчет рисков производился на основе метода по двум параметрам. Результаты расчетов позволяют наглядно увидеть, что все риски оказались неприемлемыми (в среднем от 6 до 12 по 15-ти балльной шкале). Далее были внедрены средства защиты, направленные на понижение рисков, которые были рассчитаны раньше. После выявления системы защиты информации необходимых для понижения рисков, был произведен перерасчет рисков по данному методу. В результате перерасчета рисков с учетом внедренных систем защиты информации произошло их понижение до приемлемого уровня, а именно уровень риска снизился в два раза (в среднем от 2 до 6).

Заключение

В результате проведенной работы актуальность темы была доказана. Появление MPLS открывает большие возможности при создании магистральных IP-сетей. Новая технология может значительно улучшить существующие способы их создания: как с помощью IP-маршрутизаторов, соединенных каналами «точка-точка», так и на базе транспортной сети ATM, поверх которой работают IP-маршрутизаторы.

В обоих случаях применение MPLS дает значительные преимущества. В магистральной сети ATM появляется возможность одновременно предоставлять клиентам как стандартные сервисы ATM, так и широкий спектр услуг IP-сетей наряду с дополнительными сервисами. Данный подход может существенно расширить пакет услуг, предлагаемый провайдерами, заметно повышая их конкурентоспособность на рынке. Совместное же использование IP и ATM, соединенных посредством MPLS, способствует еще большему распространению этой технологии и создает основу для построения крупномасштабных интегрированных сетей с большим набором сервисов.

Мною были разработаны схемы коммутации MPLS протокола и проанализирована устойчивость MPLS VPN к атакам. Первое, что необходимо было сделать, это включить MPLS глобально. Было применено mpls ip в режиме глобальной конфигурации. На каждом интерфейсе дополнительно активи-рован mpls.

В главе безопасность жизнедеятельности анализируются оптимальные условия труда для разработки программного обеспечения, а также определяются необходимые меры безопасности.

Цель главы анализа и оценки рисков состоит в определении характеристик рисков корпоративной информационной системы и ее ресурсов. В результате оценки рисков становится возможным выбрать средства, обеспечивающие желаемый уровень информационной безопасности компании. При оценивании рисков учитывались: ценность ресурсов, значимость угроз и уязвимостей, эффективность существующих и планируемых средств защиты. Были рассмотрены теоретические основы рисков информационной безопасности, выявлены основные способы ее оценки, также были освещены наиболее распространенные методики расчета оценки рисков информационной безопасности.

Список литературы

1. Лукацкий А. Неизвестная VPN //abn: Компьютер. 2020. URL: http://abn.ru/inf/compress/network4.shtml (дата обращения 28.03.2020).
2. Норманн Р. Выбираем протокол VPN // Windows IT Pro. 2018. URL: http://www.osp.ru/win2000/2001/07/03.htm (дата обращения 05.04.2020).
3. Петренко С. Защищенная виртуальная частная сеть: современный взгляд на защиту конфиденциальных данных / Мир Internet. – М.: №2, 2001.
4. Салливан К. Прогресс технологии VPN. PCWEEK/RE, – М.: №2, 1999.
5. Файльнер М. Виртуальные частные сети нового поколения LAN/Журнал сетевых решений, – М.: №11, 2005 http://www.osp.ru/lan/2005/11/030.htm.
6. Фратто М. Секреты виртуальных частных сетей. Сети и системы связи, №3, 1994.
7. Штайнке С. VPN между локальными сетями. LAN/Журнал сетевых решений, – М.: №3,1994.
8. Ефремова О.С. Документация по охране труда в организации. [Текст] Практическое пособие /О.С. Ефремова 5-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2015 г. – 152 с.
9. ГОСТ IEC 61140-2012. Защита от поражения электрическим током. Общие положения безопасности установок и оборудования [Текст]/ М.: Стандартинформ, 2012 – 30с.
10. Белов С.В. Безопасность жизнедеятельности. – М.: Издательство Высшая школа 1999. – 29 с.
11. СанПин 2.2.4.548-2001.Санитарные правила и нормы. Гигиенические требования к микроклимату производственных помещений [Текст] / Санитарные правила и нормы. – М.: Информационно-издательский центр Минздрава Казахстана. 2001. -20 с.
12.ГОСТ 12.1.038-82. Система стандартов безопасности труда. Электробезопасность. Предельно допустимые значения напряжений и токов [Текст] / М.: ИПК издательство стандартов, 2001-15с.
13.Ефремова О.С. Документация по охране труда в организации. [Текст] Практическое пособие /О.С. Ефремова 5-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2015 г. – 152 с.
14.Ефремов О.С. Охрана труда в организации в схемах и таблицах. [Текст] / О.С. Ефремова 7-е изд. перераб. и доп. -М.: Изд. “Альфа-Пресс”,2018 г. 124 с.
15.СанПин 2.2.4.548-2001.Санитарные правила и нормы. Гигиенические требования к микроклимату производственных помещений [Текст] / Санитарные правила и нормы. – М.: Информационно-издательский центр Минздрава Казахстана. 2001. -20 с.
16. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С. А., Симонов С. В. - М.: Компания АйТи; ДМК Пресс, 2004.- 359 с.

17. Ищейнов, В. Я. Основные положения информационной безопасности. Учебное пособие / В.Я. Ищейнов, М.В. Мецатунян. - М.: Форум, Инфра-М, 2015. - 208 с.
18. Мельников, Д. А. Организация и обеспечение безопасности информационно-технологических сетей и систем. Учебник / Д.А. Мельников. - М.: КДУ, 2015. - 598 с.
19. Сообщество системных администраторов // Litl-admin.ru: Уроки Packet Tracer. Обзор протокола ARP. URL: https://litl-admin.ru/rabota-s-setyu/uroki-packettracer-obzor-protokola-arp.html (дата обращения: 25.02.20).