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 Технологий_____
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	старший преподаватель	17.02.2020 –	

информационной безопасности	Дмитриева Маргарита Валерьевна	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 «_11_»____октября____ 2019г.

Заведующий кафедрой _____ (Бердибаев Рат Шындалиевич)
(подпись) (ФИО)

Научный руководитель проекта _____ (Шайкулова Актоты Алиевна)
(подпись) (ФИО)

Научный руководитель проекта _____ (Альмуратова Камшат Бимуратовна)
(подпись) (ФИО)

Задание принял к

исполнению студент _____ (Бекетаева Гаухар Айдарқызы)
(подпись) (ФИО)

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 подходящие условия труда сотрудников. 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 the appropriate working conditions for employees. 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.

Аңдатпа

Дипломдық жобада fpsu-IP бағдарламалық пакетінің базасында қорғалған банк желісі әзірленді, MPLS протоколының негізінде VPN-желілері әзірленді, сонымен қатар MPLS-ді қосу және дестелерді тег бойынша жіберу үшін маршрутизаторда интерфейстер теңшелген.

Өмір тіршілігінің қауіпсіздігіне арналған тарауда қызметкерлердің тиісті еңбек жағдайлары сипатталады. Тәуекелдерді талдау және бағалау тарауында қауіптердің туындау ықтималдығын азайту жөніндегі шараларды қолданғанға дейін және одан кейін тәуекел деңгейінің екі параметрлері бойынша есептер жүргізілді.

Содержание

Введение

На данный момент в мире телекоммуникаций идет повышенный спрос к виртуальным частным сетям (VPN). Причиной служит необходимость уменьшения затрат на обслуживание корпоративной сети за счет более дешевого соединения между удаленными офисами и удаленными пользователями через Интернет. На самом деле, иногда прокладывается сопоставление затрат на подключение сервиса к большому числу сеток в сети, например, к сети Frame Relay, то можно обнаружить значительную разность в цене. Впрочем существенно отметить, что при соединенье сеток Веба незамедлительно же всплывает вопрос о сохранности данных, оттого должно организовывать механизмы предоставления конфиденциальности и целостности подаваемой информации. Сети, на основе такового механизма называемые условной собственной сетью.

Кроме, нередко нашему современнику, занимающемуся вырабатыванием личного бизнеса, требуется видимо-невидимо путешествовать. Такое может существовать странствие в отдаленные уголки державы или в посторонние страны. Это не уникальность ради людей, какие располагают путь к своей информации, хранящейся для их домашнем компьютере сиречь компьютере компании. Эту проблему возможно решить, запустив отосланное формирование посредством радиомодем и телефонную линию. Применение телефонной полосы располагает свои особенности. Минусы такового заключения охватываются в том, что звонок из другой державы стоит больших денег. Для безопасного отосланного доступа, употребляется VPN. Превосходства схемы VPN охватываются в том, что организация отосланного прохода исполняется после телефонной линии, но через интернет, это очень экономичнее и лучше. На мой взгляд, разработка VPN располагает безграничный горизонт после всему миру.

1 Понятие и классификация VPN сетей, их построение

1.1 Что такое VPN

VPN организовывает безобидное формирование промежду вашим устройством (например, вашим компьютером или смартфоном) и Интернетом. Иногда мы в сети, у всех нас есть неповторимые IP-адреса. Вам продоставляется возможность сопоставить данный адресок с номером телефона или домашним адресом, но для вашего компьютера или смартфона: ваш IP-адрес - такое индивидуальный распознавательный код вашего интернет-соединения. Он показывает ваше местопребывание и связан с человеком, некоторый выплачивает вашему интернет-провайдеру. С вашим IP-адресом вы можете существовать идентифицированы и отслежены онлайн, вне зависимости от того, а вот и нет делаете. Ежели вы не используете VPN.

VPN гарантирует безопасность, поелику она неукоснительно шифрует весь ваш интернет-трафик пред того, как он добивает VPN-сервера, и направляет ваш трафик посредством значительно больше благонадежный «VPN-туннель». Это затрудняет захват и просмотр ваших предоставленных другими, в том числе правительства и хакеры . По этой первопричине настойчиво советуется утилизировать VPN, ежели вы утилизируете (опасные) общественные узы WiFi .

Впрочем возможно да располагать логос утилизировать VPN для службе сиречь дома. Поставщики, в том числе NordVPN и ExpressVPN, призывают перворазрядные ватерпасы кодирования AES 256. Вследствие данной обороне вам не имеет смысла тревожиться о том, что кто-то коллекционирует ваши материалы и утилизирует их насупротив вас.

Сам по себе принцип службы VPN не противоречит базисным сетным технологиям и протоколам. Иногда формирование отосланного прохода установлено, посетитель посылает хор пакетов в протоколе PPP, как сервер. если условных назначенных установок промежду местными сетями их маршрутизаторы да перебрасываются пакетами PPP.

Наличествующая сетная инфраструктура бражки может статься подготовлена для базе употребления условных собственных сетей, до программно-аппаратных средств. Компанию условной собственной узы возможно сопоставить с передачей предоставленных после вселенской сети. В большинстве случаев, непосредственное формирование промежду вытащенным юзером и окончательной точкой туннеля водворяется по протоколу PPP.

Преимущественно разблаговещенным способом создания VPN-туннелей представляется инкапсуляция сетных протоколов (IP, IPX, AppleTalk и т. д.). в PPP, а затем инкапсулировать пакеты, какие определяются в протокол

туннелирования. Естественно такое интернет, или (реже) банкомат и Frame Relay. Данный подъезд был назван туннелированием второго уровня.

1.2 Классификация VPN сетей

Систематизацию VPN сети возможно выработать после нескольким ключевым параметрам:

1. По принципу используемой среды:

Непроницаемые VPN узы - такое больше общераспространенный разновидностей частных собственных сетей. С его поддержкой вероятно организовать беспроигрышную и защищенную подсеть для Интернета. Образчик непроницаемых VPN являются: IPSec, OpenVPN и PPTP.

Конфиденциальные VPN сети. Употребляются в случаях, иногда передающую сферу возможно вычислять беспроигрышной и необходимо постановить исключительно задачку создания условной сабсети в масштабах огромной сети. Вопросы предоставления безопасности стопорятся неактуальными. Образчиками подобных VPN заточение являются: MPLS и L2TP. Материалы протоколы перелагают задачу компании обороны на другие, например L2TP, во множестве случаев, применяется в чете с IPSec.

2. По способу реализации:

VPN бремена на манер своеобразного программно-аппаратного обеспечения. Реализация VPN узы исполняется посредством своеобразного комплекса программно-аппаратных средств. Такая реализация гарантирует добропорядочную производительность и, во множестве случаев, добропорядочную степень защищённости.

VPN бремена на манер программного решения. Утилизируют самостоятельный принтсервер с своеобразным программным обеспечением, обеспечивающим трудоспособность VPN.

VPN бремена с интегрированным решением. Трудоспособность VPN гарантирует комплекс, радикальный конечно задачи фильтрации сетного трафика, бражки сетного экрана и предоставления качества обслуживания.

3. По типу протокола:

Присутствуют реализации относительных личных сеток вокруг TCP/IP, IPX и AppleTalk. Но на сейчас обнаруживается станция к повальному переходу для документ TCP/IP, и абсолютное большинство VPN заточений сдерживает фактически его.

4. По уровню сетного протокола:

По уровню сетного протокола на основе сопоставления с уровнями эталонной двухсеточный трансформации ISO/OSI. Условные собственные узы реализуются с применением протоколов туннелирования предоставленных посредством доступную линию Интернет-связи, и с применением протоколов туннелирования, какие шифруют материалы и переходят их из конца в конец промежду пользователями. В большинстве случаев, для создания VPN-сети

употребляются последующие ватерпасы протокола: сорокаканальный уровень, сеточный уровень, пневмотранспортный уровень.

1.3 Протоколы VPN сетей

Узы VPN сооружаются с употреблением протоколов туннелирования предоставленных посредством линию связи корпоративного использования Интернет, притом протоколы туннелирования гарантируют кодирование предоставленных и осуществляют их сквозную передачу промежду пользователями. В большинстве случаев, на сегодняшний период ради учения сеток VPN употребляются протоколы последующих уровней:

1. Сорокаканальный уровень
2. Сеточный уровень
3. Пневмотранспортный уровень.

На канальном ватерпасе могут употребляться протоколы туннелирования предоставленных L2TP и PPTP, какие утилизируют авторизацию и аутентификацию.

В настоящее время преимущественно разблаговещенным протоколом VPN представляется документ двухточечной туннельной связи или Point-to-Point Tunnelling Protocol – PPTP. Сконструирован он бражками 3Com и Microsoft дабы предоставления безобидного отосланного прохода к корпоративным сеткам посредством Интернет. PPTP утилизирует имеющиеся обнаруженные образцы TCP/IP и во многом подобает на устаревший документ двухточечной связи PPP. На поверку PPP так и остается коммуникационным протоколом сеанса составления PPTP. PPTP организовывает выработок посредством линию к NT-серверу получателя и передает по нему PPP-пакеты отосланного пользователя. Принтсервер и автоматизированное рабочее место утилизируют условную собственную линию не направляют внимания на то, сколь безобидной или доступной представляется вселенская линию промежду ними. Заключение сеанса составления после инициативы сервера, отлично от специализированных сервов отосланного доступа, разрешает админам местной узы не пропускать отосланных юзеров за границы налаженности безвредности Windows NT Server.

В соотношении от расстояния промежду налаженностями абонентскими и компьютерными сетями они делятся на общий, региональный и ограниченный уровни. Имеются всепригодные и специализированные сети. Иерархию компьютерной узы возможно сконструировать последующим манером (рисунок 1. 1).

Рисунок 1.1 - Иерархия компьютерных сетей

1.4 Понятие "туннеля" при передаче данных в сетях

Для передачи данных VPN-агенты создают виртуальные каналы между защищаемыми локальными сетями или компьютерами (канал называется "туннелем", а технология его создания называется "туннелированием"). Вся информация передается по туннелю в зашифрованном виде (рисунок 1.2).

Рисунок 1.2 – Схема VPN-туннелирования

Одной изо основных функций VPN-туннеля представляется крупнопакетный фильтр. Фильтрация пакетов исполняется с поддержкой VPN-агента, опции какого не касаясь частностей представляются политикой безвредности условной собственной сети. Для увеличения безвредности условных собственных сеток в туннелях употребляются брандмауэры, и различные приборы (фильтры).

Зад безвредности – VPN-это сетное устройство, какое водился подключено к двум сеткам - wan и lan-соединениям, и должен проделывать функции кодирования и аутентификации компьютеров, размещенных после

данным шлюзом. VPN-портал возможно существовать реализован как отдельное аппаратное устройство, например из решений, и нечто вроде брандмауэра сиречь маршрутизатора, наращенного способностями VPN.
Сторону охватывается в том, что эта разработка разрешает зашифровывать первобытный мешок целиком, совместно с заголовком, но не исключительно материалы в поле. Первобытный мешок кодируется полностью, совместно с заголовком и зашифрованным свертком вмещается внутри прочего наружного пакета, дабы обнаружить заголовок. Передача предоставленных из "опасной" узы и обнаруженных филиалов наружного пакета да употребляется при появлении наружного пакета, в точке его защитного канала они вытаскивают моральный пакет, дешифрование и применение заголовка для будущей передачи, ведь даже в обнаруженном варианте по сетке, не требует обороны (рисунок 1. 4).

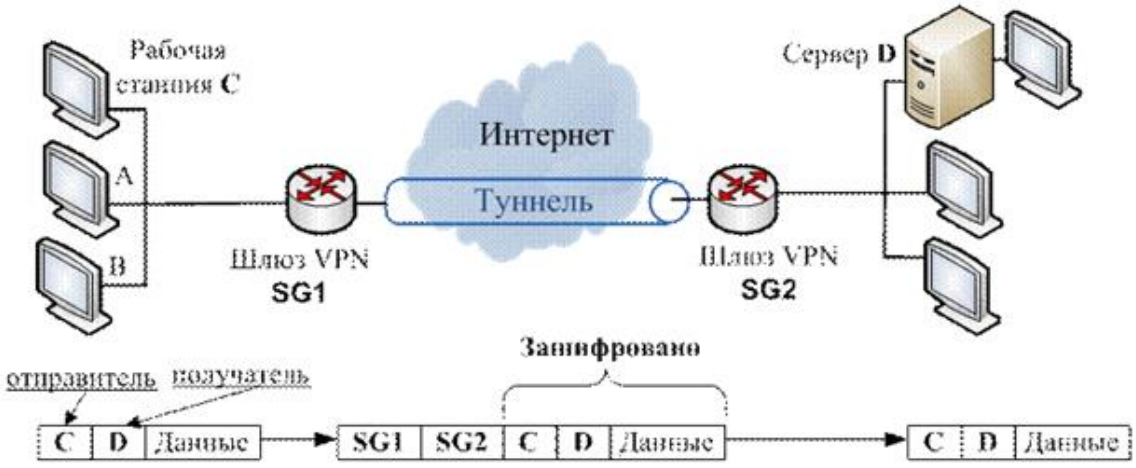


Рисунок 1.4 - Организация туннеля VPN

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).

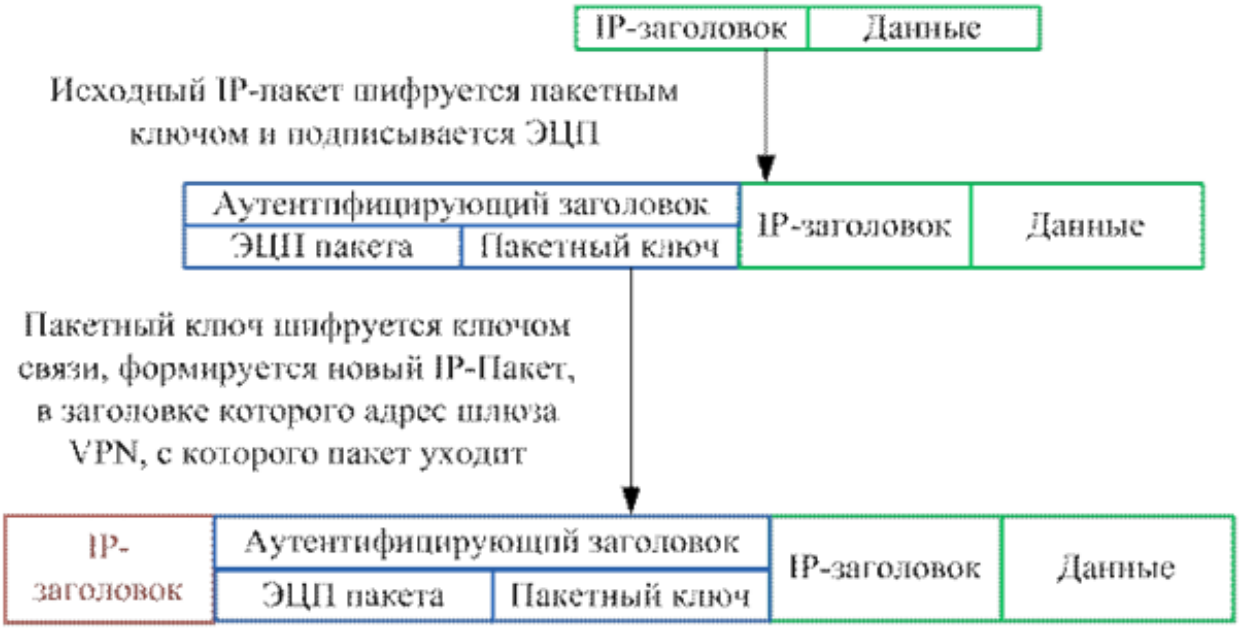


Рисунок 1.5 - Туннелирование пакетов

1.5 Виды архитектуры VPN-сетей

С помощью схемы (рис. 1.6) 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.

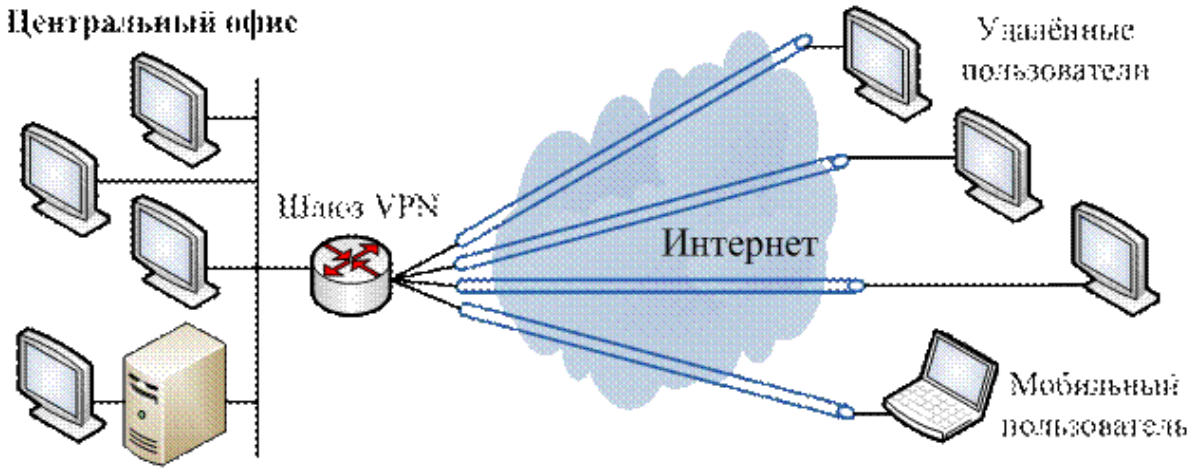


Рисунок 1.6 - VPN с удалённым доступом

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 будет доступ на ресурсе "родительской" компании, а также для обмена информацией друг с другом (рисунок 1.7).

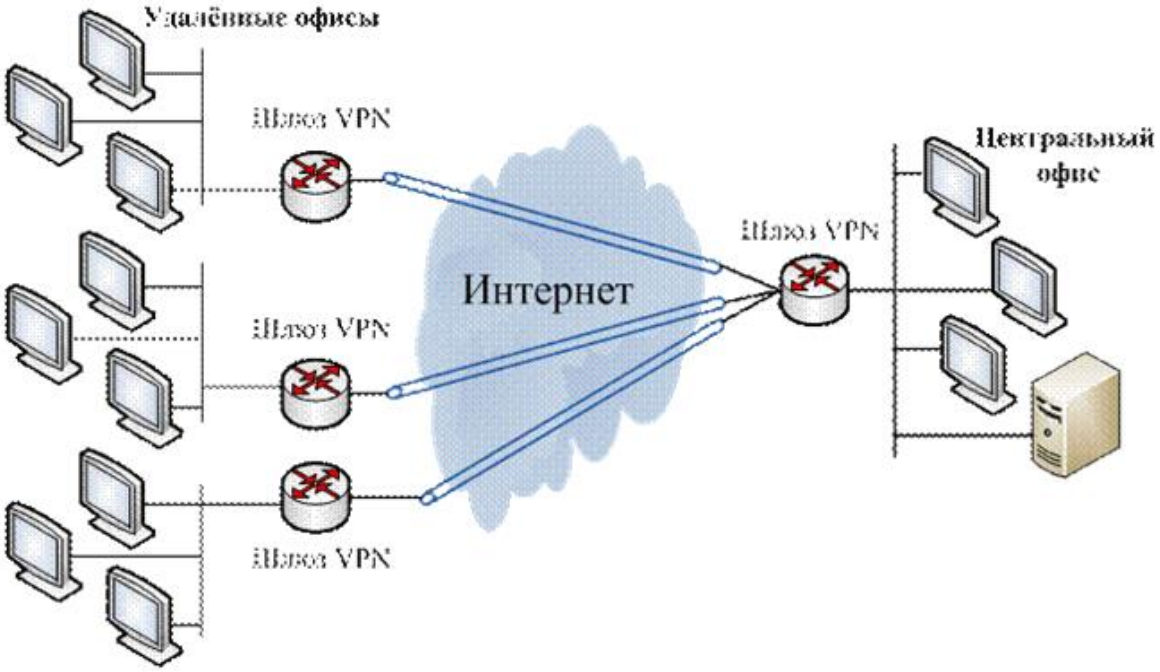


Рисунок 1.7 - Intranet VPN

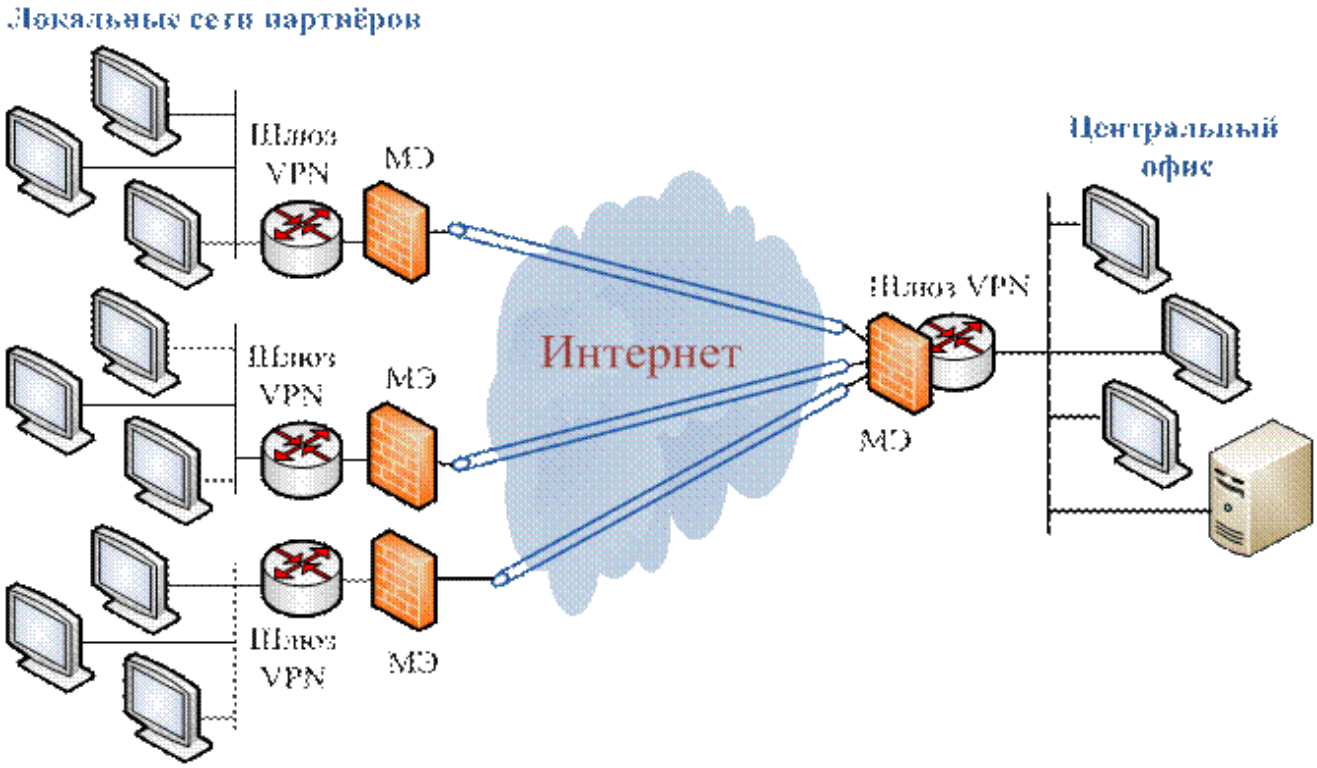


Рисунок 1.8 - Extranet VPN

Программно-аппаратный комплекс ФПСУ-IP представляется программно-техническим лекарством обороны через неразрешенного прохода к информации. Комплекс осуществляет функции межсетевого экрана и учения условных собственных сеток поверху вселенских и локальных вычислительных сетей. В составе ФПСУ-IP употребляется состояние шифровальной обороны информации, что дает возможность реализовывать кодирование подаваемой информации.

Многофункциональные способности программно-аппаратного ансамбля "ФПСУ-IP" после обороне через НСД могут существовать расширены последующими раздельными изделиями:

1. программно-аппаратный комплекс "ФПСУ-IP/Клиент", апперципируемый в персонал отосланных пролетариев станций для высокой защиты их подключений к защищенным "ФПСУ-IP" местным сетям;
2. Комплекс "ЦВК", созданный для выработки ключей парно-выборочной связи, употребляемых "ФПСУ-IP";
3. программно-аппаратный комплекс "Удаленный руководитель ФПСУ-IP" (далее УА ФПСУ-IP), созданный для дистанционного контроля и управления категорией "ФПСУ-IP";
4. Кода "Центр генерации ключей клиентов", созданная для создания первостепенных систем обороны размена предоставленными промежду юзерами "ФПСУ-IP/Клиент" и "ФПСУ-IP".

"ФПСУ-IP" аппаратно подключается в проход оковы промежду обороняемой сферой другой частично местной узы четой физиологических установок (одна к обороняемой области, прочая к другой сети) следовательно, дабы всегда укладывающиеся и распространяющиеся изо площади потоки предоставленных штудировали посредством "ФПСУ-IP". Ежели сторону объединена с сетью больше чем в одной точке (транзитная область), "ФПСУ-IP" соответственны существовать поставлены на каждом выходе изо неё.

Генеральная цель "ФПСУ-IP" охватывается в том, что в согласованье с поставленными админом предписаниями он рассматривает укладывающиеся и исходящие пакеты предоставленных IP-протокола после совокупности критериев, контролирует прохода к ресурсам узы и определяет вероятность передачи данных.

На начальном рубеже разбора все пакеты, прибывающие для любой из интерфейсов "ФПСУ-IP", испытываются для вопрос корректности их формата и соответствия эталонам палочка IP-протоколов. Ежели изначальная переработка пакета исполнена успешно, мешок будет вручен ради разбора в подсистему фильтрации "ФПСУ-IP".

Фильтрация пакетов IP-протокола, вырабатываемая "ФПСУ-IP", охватывается в сравненье растений IP-пакета поставленным админом правилам. Вследствие сооруженного разбора решается о допустимости последующей передачи пакета абоненту-получателю, о необходимости последующей идентификации и аутентификации пакета, и про методы передачи предоставленных и способах контроля после процессом приёма/передачи данных.

Подневольности через топологии узы и от условий политики безвредности компании вероятны порядочно вариантов использования "ФПСУ-IP" (функциональные схемы повергнуты ниже) и всевозможные режимы его работы.

Обычнейшем случае перевод IP-пакетами абонентов сектора ЛВС с прочими абонентами возможно производиться посредством один "ФПСУ-IP" (рисунок 1. 9). Для оконечной площади довольно определить один "ФПСУ-IP" для выхода из неё, для транзитной области.

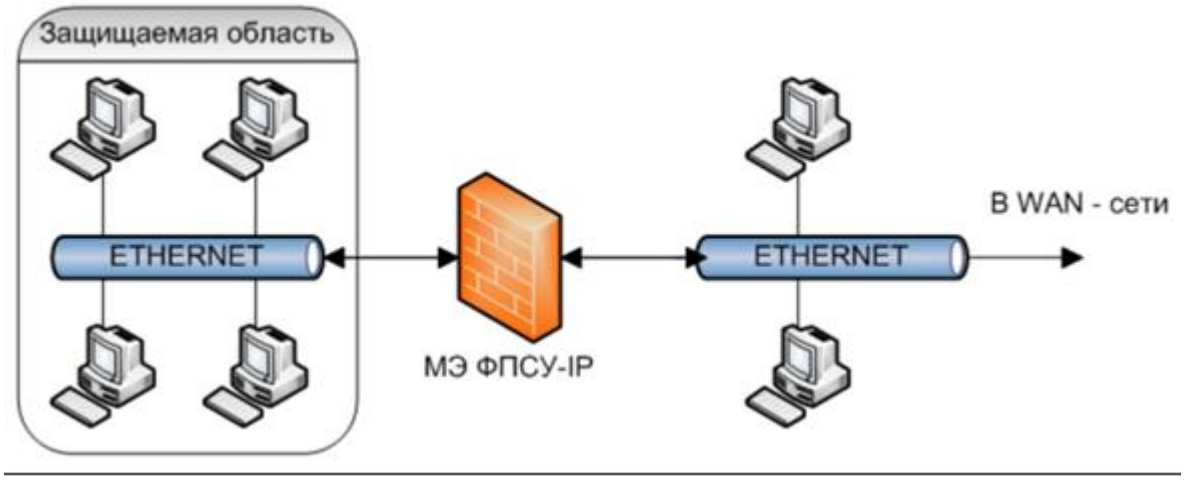


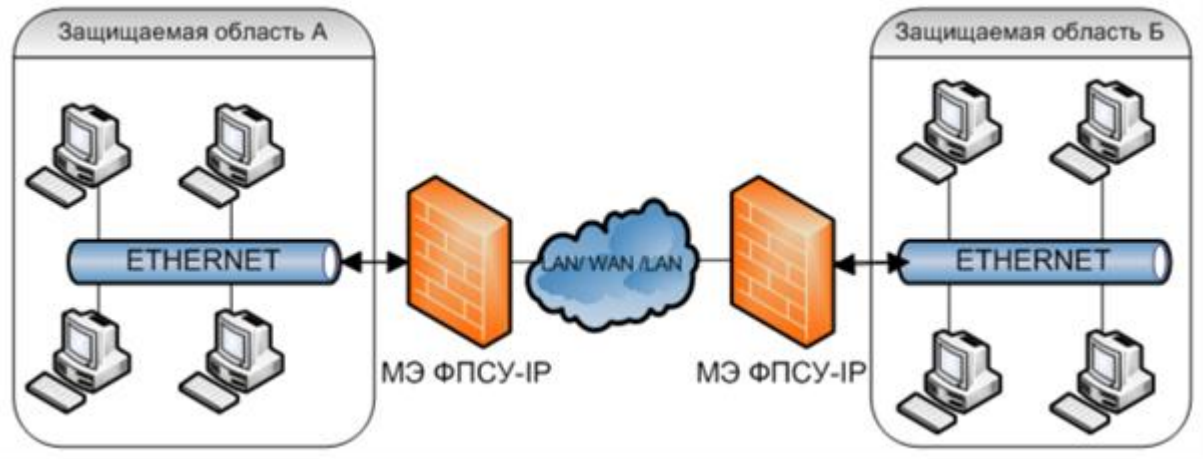
Рисунок 1.9 - Функциональная схема использования только одного "ФПСУ-IP" для защиты области.

Следовательно, из локальной узы акцентируется команда абонентов (защищаемая область), для которых перевод IP-пакетами с остальными абонентами узы может статься специфическим манером регламентирован и проконтролирован. Употребляя "ФПСУ-IP" по этой схеме, возможно разъединить местную линию на две доли (не переменяя около данном IP-адресов и установок сетного программного предоставления хостов), одна изо каких защищена, а абонентам иной будет разрешён обыкновенный перевод пакетами. По этой же схеме возможно определить "ФПСУ-IP" для выходе изо местной узы в удалённые узы и предохранить службу всей местной сети.

Ежели перевод пакетами абонентов будет изготавливаться посредством один "ФПСУ-IP", может статься реализован исключительно наислабейший уровень защиты, мнимый распорядок ретрансляции, при котором будут

задействованы исключительно механизмы фильтрации пакетов по различным критериям.

Больше торжественный уровень обороны вероятен около размене пакетами посредством два подобных "ФПСУ-IP", функционирующих в паре. Тут-то строю подсоединяются механизмы аутентификации абонентов непроницаемых сегментов ЛВС и трансляции их сетевых адресов, укрывающей внутренние адреса субъектов и объектов передачи, и используемых ими сетных протоколов и прикладных функций обороняемой сети. Кроме, в таком строю могут существовать использованы механизмы сжатия, кодирования и туннелирования.



Предоставленная программа использования разрешает использовать весь ссужаемый ансамблем комплект лекарств обороны через НСД. Впрочем она не имеет возможности гарантировать совершенную безобидность размена пакетами в случае, ежели ради кое-каких абонентов обороняемых площадей разрешены обнаруженные составления (через один "ФПСУ-IP" в режиме ретрансляции кроме аутентификации) с абонентами сиречь сетными услугами посредством вселенскую сеть.

Ежели обнаруженные составления всё же необходимы для доступа к разнообразным утилитам и сервисам Интернет, гарантировать безобидность обороняемой площади возможно последующими способами:

Вышвырнуть после величины обороняемой площади злонамеренно обособленный хост (хосты), с которого (которых) будет производиться обыкновенная пахота после Интернет, а остальным абонентам в конфигурации ансамбля определить распорядок службы посредством удалённый "ФПСУ-IP".

На "ФПСУ-IP", позволяющем кое-каким абонентам обнаруженные соединения, организовать закономерную группу, к которой будут приписаны абоненты с подтвержденными безоговорочно адресами, а на компьютерах данных абонентов приобрести меры после предупреждению пуска программ сиречь отрывков кода, общепринятых изо сети.

Изолировать чрезвычайно величественные хосты в защищаемой терминальной площади очередным "ФПСУ-IP", функционирующим в "каскадном" строю с первым, причём для втором "ФПСУ-IP" обязаны быть воспрещены всегда обнаруженные соединения. Следовательно, локалка будет раздроблена на две части, располагающие несходный уровень защиты.

Последовательная станция много "ФПСУ-IP" и запрет обнаруженных составлений на последнем ансамбле основывают большой уровень обороны ради терминальной площади (область А на рисунок 1.10), предоставляя путь к ней исключительно аутентифицированным абонентам. При всем при этом система фильтрации создаёт довольно торжественный уровень обороны через НСД и для абонентов временной обороняемой площади В, дозволяя им реализовывать составления с абонентами прочих сеток (не защищённых) посредством вселенскую сеть. Отметим, что для абонентов терминальной площади фильтрация пакетов после всем установленным аспектам будет изготавливаться исключительно кратчайшим комплексом, а транзитный "ФПСУ-IP" будет выбирать пакеты исключительно после IP-адресам.

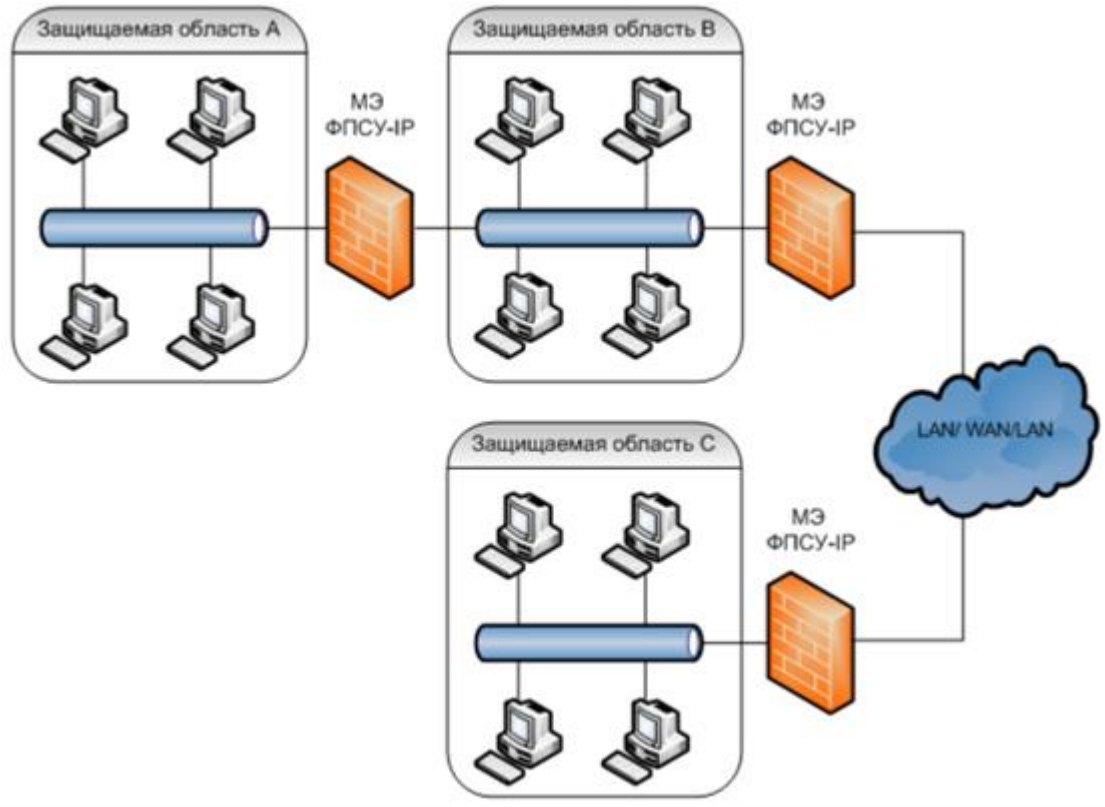


Рисунок 1.10 - Каскадная установка двух "ФПСУ-IP" в защищаемой области.

УА ФПСУ-IP в том числе специализирован для накопления и отображения информации о пребыванье оформленных "ФПСУ-IP", и для автоматического разбора данной информации с мишенью извещения админа о пришествии для "ФПСУ-IP" строя событий. Подавленность УА ФПСУ-IP для

случившееся явление возможно подсоединять в себя вывод на экран сигнала графичного отображения, голосовую сигнализацию (каждому образу действия возможно существовать зажулен исключительный эвфонический сигнал), выступление извещения на указанный адресок электрической почты, картель иной программы (указывается конец к выполняемому файлу).

Прогноз происшествий на "ФПСУ-IP" возможно производиться как в самодействующем строю с установленными админом около регистрации частотами опроса, аналогично в режиме непринужденного извлечения информации после спросу администратора. Преимущество для допрос состояния "ФПСУ-IP" бессознательны предоставляется всем оформленным для нём администраторам.

Узел прогноза выдает админу последующие возможности:

• графическое отражение информации, о случившихся на "ФПСУ-IP" событиях;

• быстрый разбор спрашиваемого ради контроля сиречь управления "ФПСУ-IP" курсором "мыши";

• немедленное приобретение информации о пребыванье подобранного "ФПСУ-IP" нажатием клавиши "мыши";

• быстрый проход в режим сетного составления с выбранным "ФПСУ-IP" ради воплощения вразумительных удалённому админу усилий после контролю и управлению "ФПСУ-IP";

• IP-адрес "ФПСУ-IP";

• состояние VPN-туннеля с данным "ФПСУ-IP" в пункт заключительного воззвания к нему УА ФПСУ-IP;

• программирование резонанса на ряд происшествий (выбор их из предлагаемого списка), на которые спрашивается безотлагательная подавленность администратора, для графической, эвфонический сигнализации (возможность подбора для каждого действия своего голосового сигнала).

Информация, отображаемая схематически на экране монитора ради всех "ФПСУ-IP", включает:

• информацию о пребыванье "ФПСУ-IP": водились ли они опрошены и работают ли в повседневный пункт времени;

• графическое отражение (и голосовую сигнализацию) запрограммированных админом эксплуатационных извещений о кое-каких событиях, приключившихся для "ФПСУ-IP".

При вызове определенных информативных окошек ради любого изо подконтрольных "ФПСУ-IP" руководитель возможно унаследовать последующие данные:

• разницу в свидетельствах целых времен "ФПСУ-IP"и УА ФПСУ-IP;

• время заключительного опроса "ФПСУ-IP" подсистемой мониторинга;
• накопленную с определённого медли информацию после оформленным для предоставленном "ФПСУ-IP" событиям: обилие изменений его конфигурации (как локальными, аналогично удалёнными администраторами), обилие запусков подсистемы фильтрации, обилие дистанционных конструкций предоставленных аутентификации, обилие изменений медли (как в автоматическом режиме, аналогично по приказу удалённого администратора), обилие конструкций дополнений/изменений к ПО и пункт протекающей версии ПО;
• накопленную с определённого медли информацию о пребыванье портов "ФПСУ-IP": тип подключённых к портам установок связи, положение установок на день заключительного опроса, поспешность передачи предоставленных после установкам для пункт заключительного опроса, время заключительных способа и передачи предоставленных по каждой линии, обилие общепринятых и переданных предоставленных в байтах и IP-пакетах после всякой линии, обилие отказов в передаче пакета и обилие нарушений верховодил фильтрации по каждой линии.
• информацию после протекающей службе "ФПСУ-IP", получаемую в строю непринужденного соединения: по состоянию его VPN-туннелей с другими "ФПСУ-IP", по состоянию службы абонентов и клиентов посредством переданный "ФПСУ-IP", по состоянию портов ансамбля и его ARP-таблиц, по работе удалённых администраторов, и материалы обо обновлениях После "ФПСУ-IP" и протекающем проценте загрузки ЦПУ;
• информацию о приключившихся в подсистеме удалённого администрирования действиях с указанием даты, медли и варианта операции.

Руководитель возможно предопределить эксплуатационную графичную и голосовую реакцию УА ФПСУ-IP высшей марки прейскурант происшествий подконтрольных "ФПСУ-IP" (соответствующие кратковременные и количественные объемы да высокомерничаются администратором),

Доскональные извещения по использованию прогноза и представление интерфейса держатся в начальстве отосланного админа "ФПСУ-IP".

2 Организация архитектуры VPN-сетей

В практической части дипломной работы была описана разработка защищенной сети Банка на основе программно-аппаратного комплекса ФПСУ-IP. Программно-аппаратный комплекс ФПСУ-IP представляется программно-техническим лекарством обороны через неразрешенного прохода к информации. Комплекс осуществляет функции межсетевого экрана и учения условных собственных сеток поверху вселенских и локальных вычислительных сетей. В составе ФПСУ-IP употребляется состояние

шифровальной обороны информации, что дает возможность реализовывать кодирование подаваемой информации.

ФПСУ-IP сконструирован для применения в вычислительных сетях, использующих магазин протоколов TCP/IP и среду передачи предоставленных Ethernet (тип кадра Ethernet_II). ФПСУ-IP представляется специальным программно-аппаратным устройством, соединяющим в себе функции межсетевого экрана, стопочного коммутатора сетного ватерпаса и организатора условных собственных сетей(VPN) поверху местных и вселенских вычислительных сетей. ФПСУ-IP аппаратно водворяется для выходе изо обороняемой местной узы в корпоративные узы и осуществляет высокоскоростную фильтрацию передаваемых пакетов данных, рассматривая их по совокупности критериев и приобретая постановление о возможности их дальнейшей передачи. Яко критериев фильтрации могут навертываться IP-адреса отправителей и получателей пакетов, допустимые номера IP-протоколов, номера портов TCP/UDP, веяние передачи пакета, время службы и разрешённые теплые связи промежду определенными абонентами. Следовательно, ФПСУ-IP разрешает реализовать осмотр и управление потоками информации, и их коммутацию из одной местной узы в другую, что отлично обеспечивает разъединение прохода и защиту сегментов ЛВС от атак злоумышленников.

Генеральная цель ФПСУ-IP охватывается в том, что в согласованье с поставленными админом предписаниями он рассматривает укладывающиеся и исходящие пакеты предоставленных IP-протокола после совокупности критериев, контролирует прохода к ресурсам узы и определяет вероятность передачи данных. На начальном рубеже разбора все пакеты, прибывающие для любой из интерфейсов ФПСУ-IP, испытываются для вопрос корректности их формата и соответствия эталонам палочка IP-протоколов. Ежели изначальная переработка пакета исполнена успешно, мешок будет вручен ради разбора в подсистему фильтрации ФПСУ-IP.

Фильтрация пакетов IP-протокола, вырабатываемая ФПСУ-IP, охватывается в сравненье растений IP-пакета поставленным админом правилам. Вследствие сооруженного разбора решается о допустимости последующей передачи пакета абоненту-получателю, о необходимости последующей идентификации и аутентификации пакета, и про методы передачи предоставленных и способах контроля после процессом приёма/передачи данных.

Приспосабливаемый "ФПСУ-IP" механизм контроля передачи пакетов на сетевом ватерпасе разрешает задавать в свойстве критериев фильтрации: • регистрационные материалы ансамблей "ФПСУ-IP/Клиент";

- IP-адреса и MAC-адреса отправителя и получателя;
- допустимые режимы службы абонентов;

- период недели и время соединения;
- используемые порты TCP и UDP соединений;
- используемые протоколы автотранспортного уровня;
- допустимые теплые связи абонентов и клиентов. В соотношении от топологии узы и от требований политики безвредности компании вероятны порядочно вариантов использования "ФПСУ-IP" и различные режимы его работы.

Под удаленным проходом к ресурсам ИС Жестянка разумеют любые виды доступа, исполняемые после внутренним и наружным каналам связи.

Вариантом отосланного прохода является:

- путь к корпоративной узы после коммутируемым каналам связи с употреблением телекоммуникационного оборудования, ссужаемый адептам компаний-партнеров, колпачащих службы в корпоративной узы Банка, единодушно исподней схеме;
- путь компании-партнеру ради прогноза службы устройств самообслуживания Банка, единодушно исподней схеме.

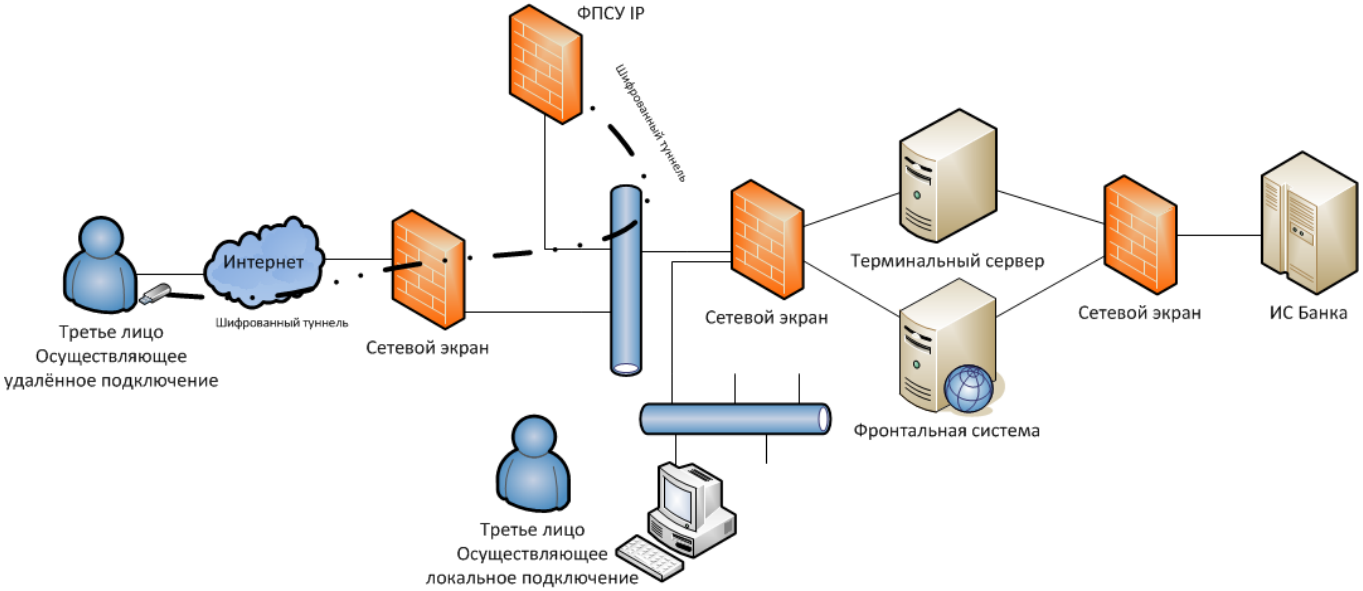


Рисунок 2.1- Схема защищенной сети

Доступ к ресурсам предоставляется после открытия сетевых доступов:

- от IP клиента до IP ресурса;
- по портам используемых протоколов (443, 80, 3389 и так далее);
- далее учитывается авторизация сотрудника в информационных системах, используя службы сертификации Банка.

Для предоставления удаленного доступа сотрудникам выдается настроенный ФПСУ-ключ (токен) с индивидуальным ip-адресом,

инициализируемый перед выдачей и привязывается к сотруднику, который данный ключ будет использовать через программу ФПСУ IP клиент.

Ключ на личной рабочей станции сотрудника активируется после ввода пин кода (рисунок 2.2).

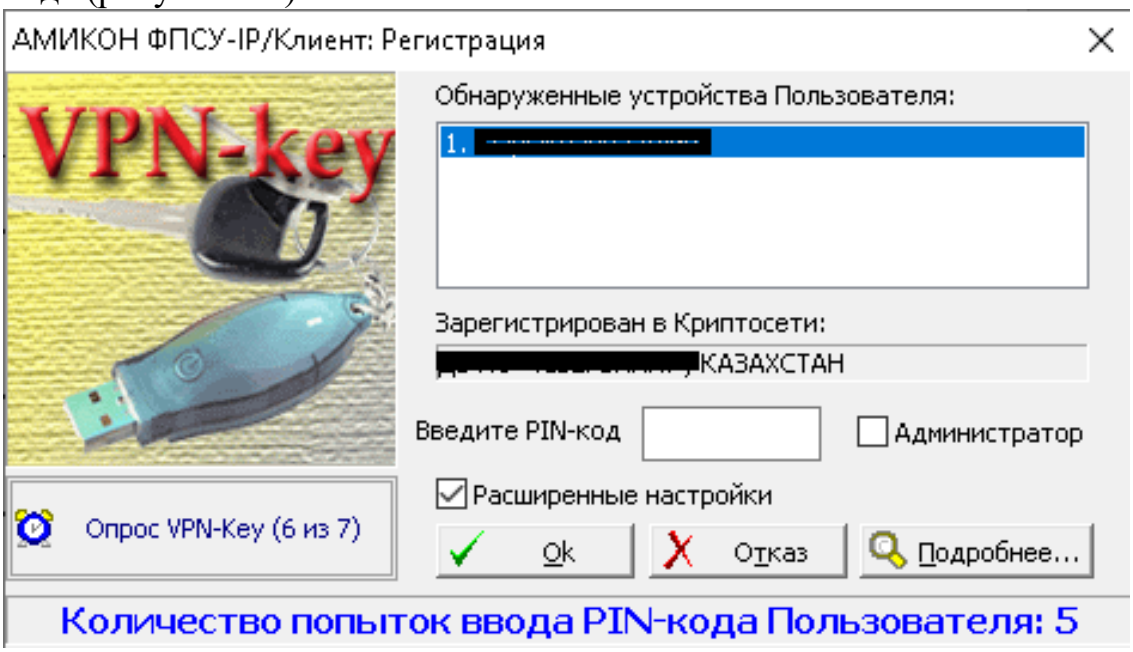


Рисунок 2.2 – Окно авторизации

Далее будут представлены настройки удалённого подключения для ФПСУ ключей на сервере ФПСУ-IP.

Поле маршрутизаторы предназначено для ведения на ФПСУ-IP описателей маршрутизаторов, через которые могут быть доступны абоненты или другие ФПСУ-IP.

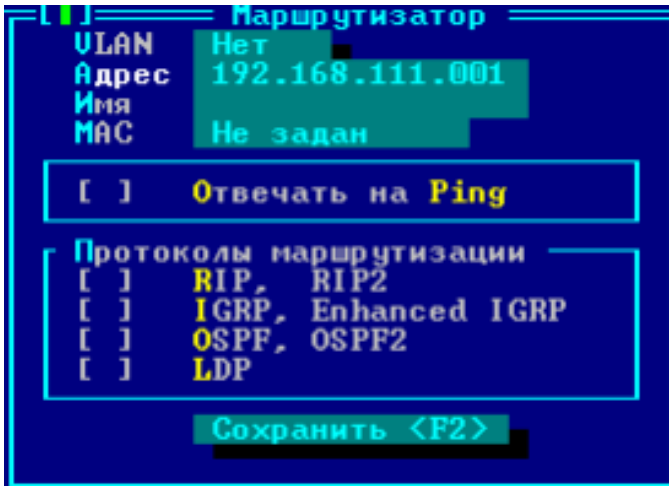


Рисунок 2.3 – Поле маршрутизатор

К каждому ключу добавляются правила, в зависимости от бизнес-требований.

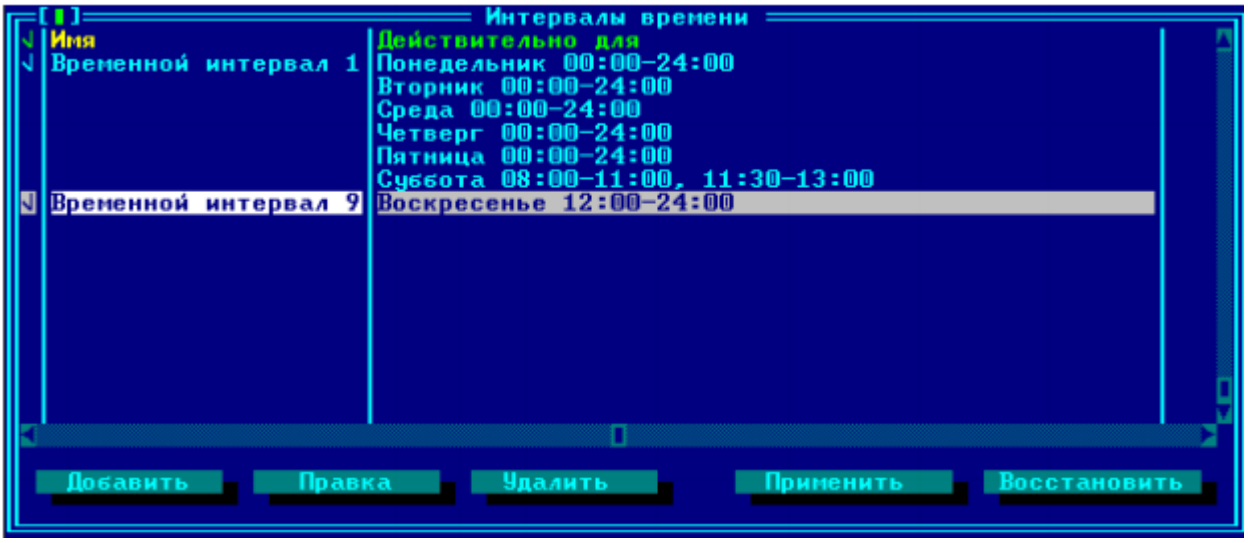


Рисунок 2.4 – настройка интервалов времени работоспособности ФПСУ ключа

Для каждого дня недели можно указать до четырех временных интервалов, в которые разрешен обмен пакетами. Если ограничений нет - устанавливается интервал 00:00 - 24:00, если работа не разрешена - временные интервалы остаются пустыми.

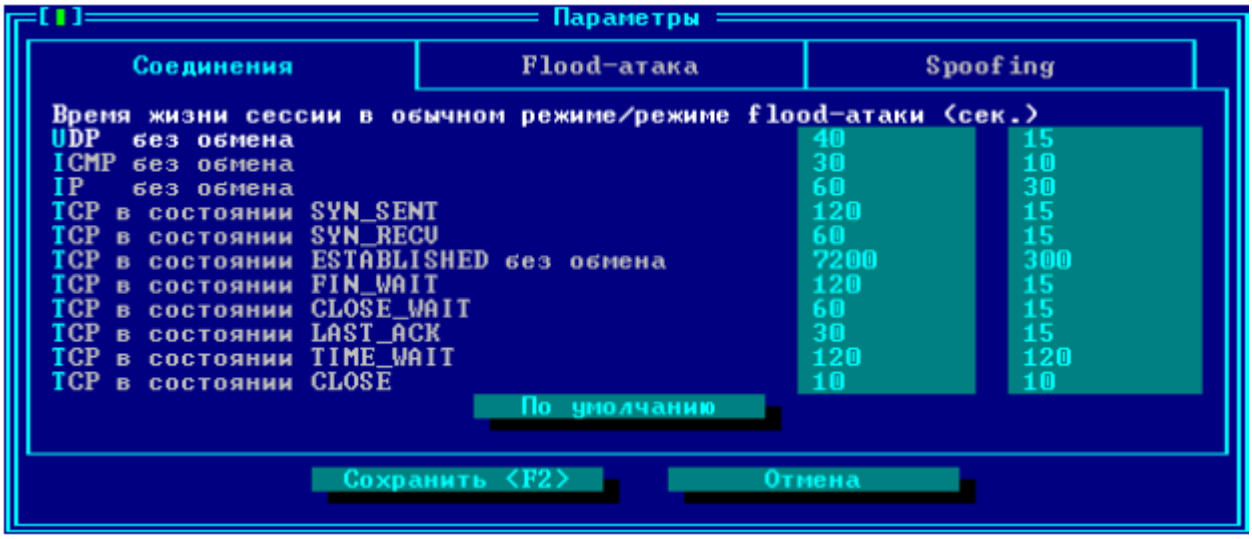


Рисунок 2.5 – Настройка времени сессии по протоколам

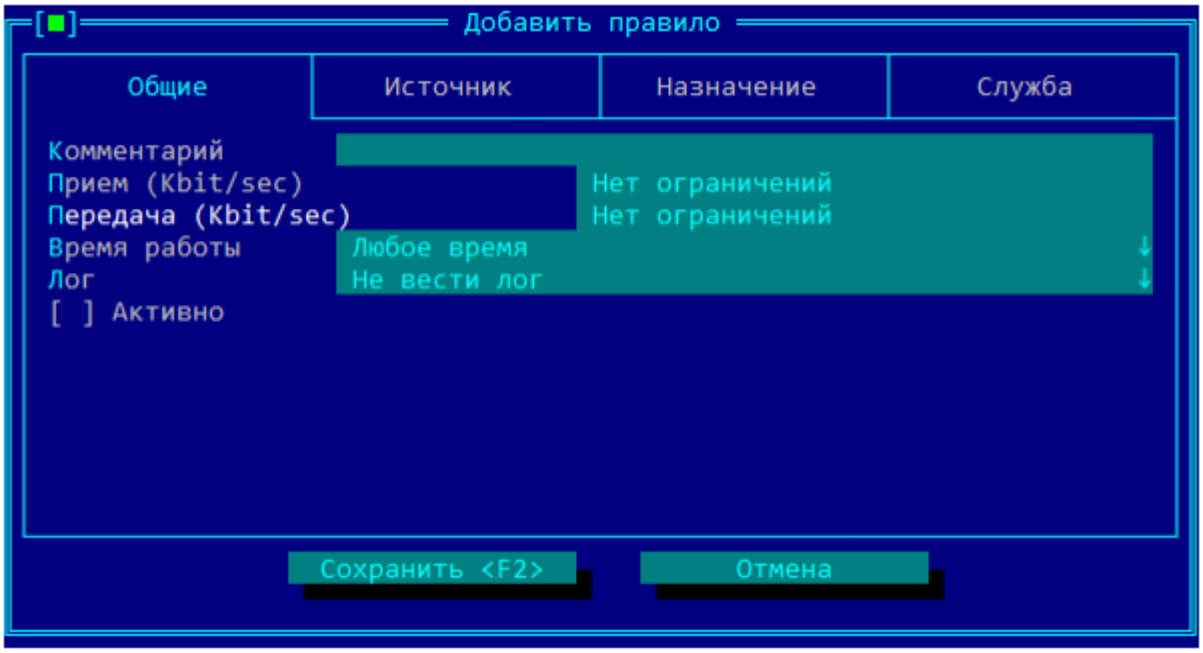


Рисунок 2.6 – Настройка ограничений передаваемых и принимаемых пакетов

Для того чтобы указать подсистеме защиты каналов управления маршрутизаторами абонентов, которые получат доступ к управлению текущим маршрутизатором, отмечается курсором нужный маршрутизатор (рисунок 2.7).

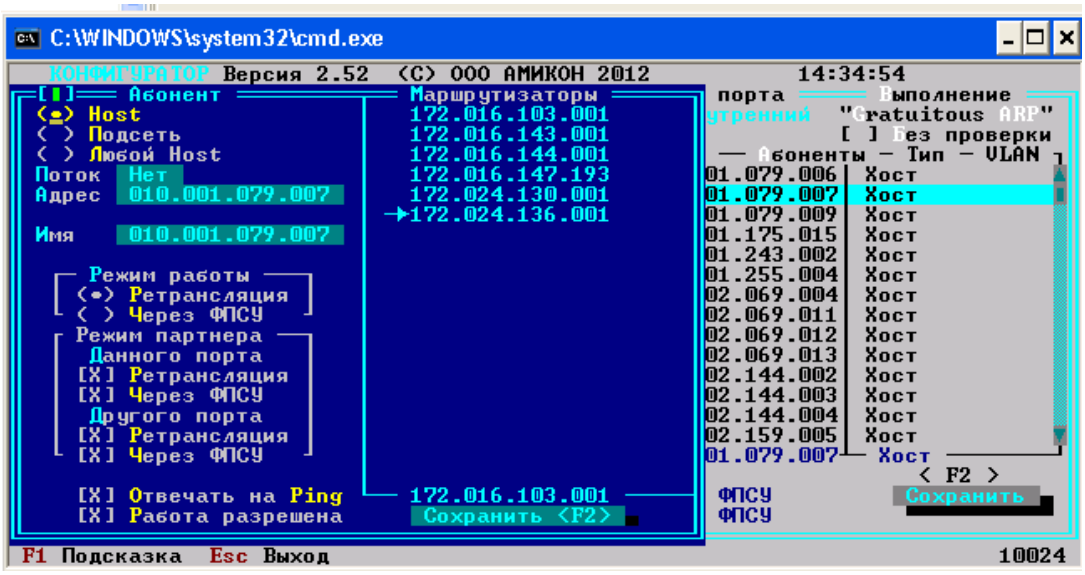


Рисунок 2.7 –Доступ хостов к подсетям ФПСУ ключей

По рисунку 2.7 можно увидеть настройку хостов ресурсов, до которых необходим доступ через ФПСУ ключ, если сотрудник будет запрашивать доступ к хосту, который относиться к маршрутизатору из другой подсети, ресурс не будет доступен. Данная конфигурация сохраняется у ФПСУ ключей, доступ к которым прописан по IP адресам и портам к хосту, что позволяет производить более защищенное соединение.

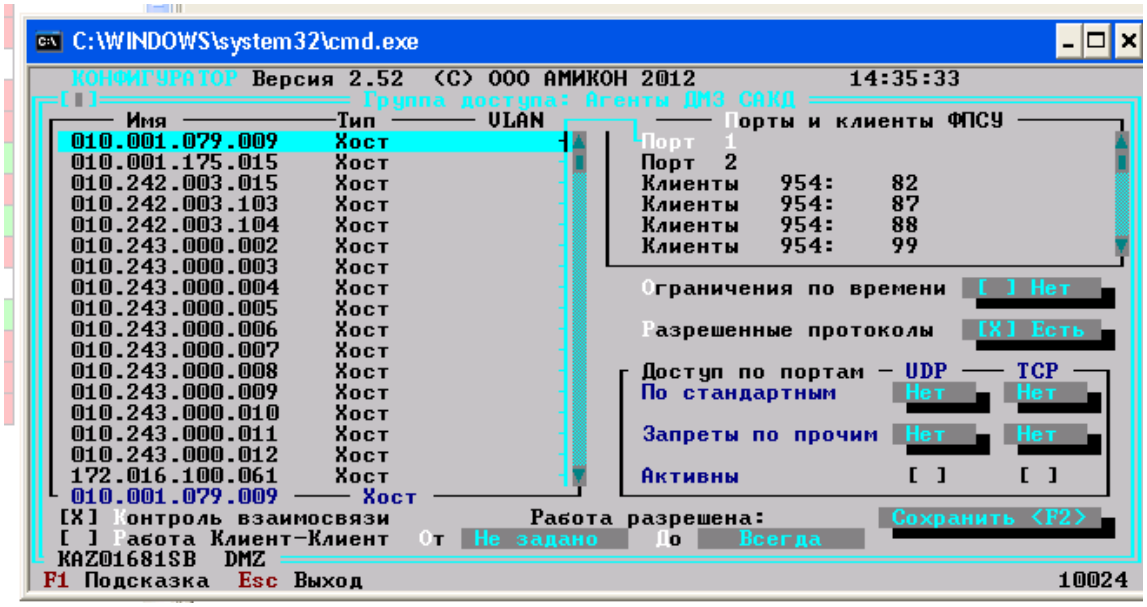


Рисунок 2.8 – Список хостов и портов

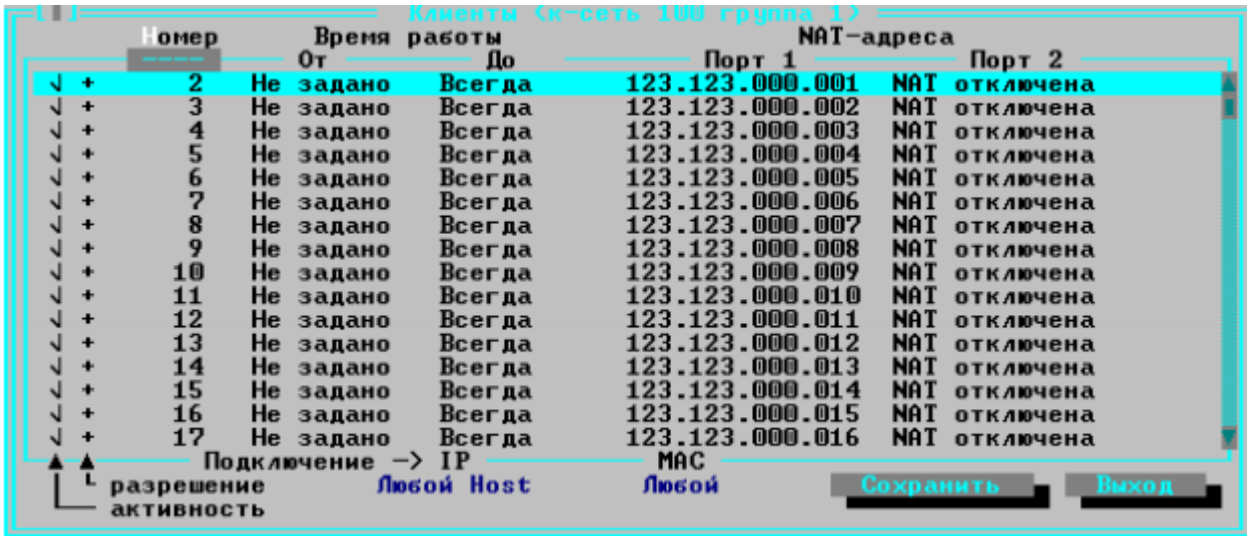


Рисунок 2.9 - Список зарегистрированных в группе Клиентов

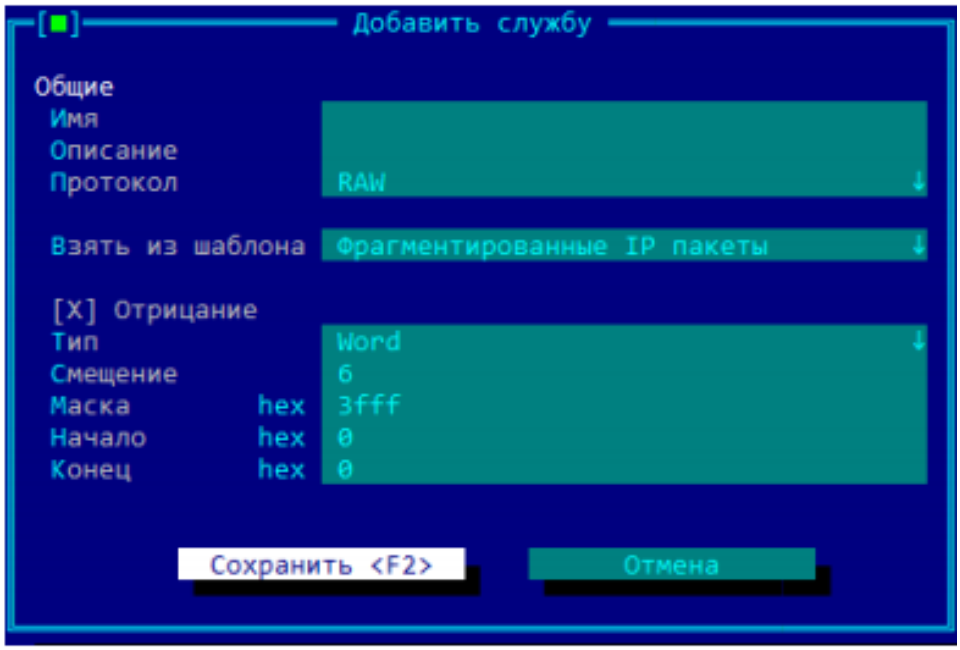


Рисунок 2.10 - Фильтра фрагментированных IP-пакетов

При добавлении данной службы к правилу фильтрации трафика по содержимому межсетевого экрана ФПСУ-IP, у которого основным действием с пакетами является Drop, будут скинуты все пакеты, идущие от источника, в IP-заголовке которых установлен признак фрагментации передаваемых данных.

№ клиента	NAT IP адрес	IP клиента	Передано байт	Принято байт	Ош	Время соединения	Последний обмен	По
00954.00120.00023	172.024.139.069	185.097.114.149	10468839	6131922		05.05.2020 09:12:38	05.05.2020 10:58:14	
00954.00120.00026	172.024.139.072	090.143.032.125	238218	129261		21.04.2020 09:25:50	21.04.2020 09:26:30	
00954.00120.00037	172.024.139.073	095.082.124.167	54619	143905		05.05.2020 09:38:38	05.05.2020 09:58:46	
00954.00127.00007	172.024.139.074	147.030.047.140	23471739	907142		07.04.2020 07:33:02	07.04.2020 07:45:54	
00954.00120.00040	172.024.139.077	081.088.147.034	9423501	268926		03.04.2020 18:55:38	03.04.2020 19:09:50	
00954.00120.00041	172.024.139.078	213.109.220.178	18813770	859499		03.04.2020 12:30:12	03.04.2020 12:45:22	
00954.00120.00043	172.024.139.080	037.150.004.062	0	0		30.03.2020 16:20:22	30.03.2020 16:28:54	
00954.00120.00044	172.024.139.081	085.117.097.072	4740122	82234		01.04.2020 23:16:46	01.04.2020 23:21:12	
00954.00120.00064	172.024.139.083	081.088.154.075	0	1088		05.05.2020 09:44:36	05.05.2020 09:46:46	
00954.00127.00114	172.024.139.085	005.250.134.054	67271039	3542129		04.05.2020 09:32:56	05.05.2020 00:04:38	
00954.00120.00048	172.024.139.087	178.091.019.122	16233207	438021		10.04.2020 08:01:04	10.04.2020 08:04:34	
00954.00120.00052	172.024.139.091	002.133.076.113	2716252	163552		27.04.2020 01:37:10	27.04.2020 01:41:50	
00954.00120.00054	172.024.139.093	002.073.158.104	17287113	408813		30.03.2020 18:33:48	30.03.2020 18:58:24	
00954.00120.00058	172.024.139.097	178.089.099.003	7130111	2542612		05.05.2020 08:47:20	05.05.2020 10:58:18	
00954.00120.00106	172.024.139.099	213.109.220.110	5359314	58689		28.03.2020 15:16:12	28.03.2020 15:17:06	
00954.00127.00136	172.024.139.100	005.076.215.236	146988163	19484196		05.05.2020 08:58:36	05.05.2020 10:58:18	
00954.00120.00065	172.024.139.104	185.097.114.149	2327253649	28191042		06.04.2020 11:51:16	06.04.2020 12:41:20	
00954.00120.00066	172.024.139.105	005.251.161.199	52202276	12744115		27.04.2020 18:03:34	27.04.2020 20:17:00	
00954.00120.00067	172.024.139.106	095.082.116.062	5150666	3108146		30.04.2020 11:04:54	30.04.2020 11:30:56	
00954.00120.00068	172.024.139.107	095.082.120.085	3577157	612064		29.04.2020 15:51:10	29.04.2020 15:57:44	
00954.00120.00069	172.024.139.108	213.109.221.075	43518689	8730605		05.05.2020 09:08:56	05.05.2020 10:58:18	
00954.00120.00070	172.024.139.109	213.211.090.018	51523373	27686559		04.05.2020 20:49:06	05.05.2020 10:58:18	
00954.00120.00072	172.024.139.112	095.082.116.181	31524144	12078338	+	04.05.2020 22:38:10	04.05.2020 23:30:44	
00954.00120.00079	172.024.139.115	081.018.033.228	168444	142025		06.04.2020 15:14:40	06.04.2020 15:15:30	
00954.00120.00134	172.024.139.116	090.143.045.180	16218932	369885		17.04.2020 06:53:32	17.04.2020 06:58:02	
00954.00120.00076	172.024.139.117	067.209.131.132	13333729	2635288		03.05.2020 16:36:14	03.05.2020 16:56:12	
00954.00120.00080	172.024.139.118	095.082.116.152	3568760	831742		29.04.2020 09:36:20	29.04.2020 09:52:20	
00954.00120.00092	172.024.139.121	095.057.117.041	4269958	462746		31.03.2020 12:00:52	31.03.2020 12:03:28	
00954.00120.00093	172.024.139.122	095.056.208.022	34315743	5755945		05.05.2020 08:16:18	05.05.2020 10:58:18	
00954.00120.00095	172.024.139.124	090.143.024.082	1	672		29.03.2020 15:50:34	29.03.2020 16:13:28	
00954.00120.00096	172.024.139.125	090.143.017.146	2595445	763747		16.04.2020 20:23:08	16.04.2020 20:40:18	
00954.00120.00098	172.024.139.127	090.143.024.154	436992	22480		04.04.2020 04:17:12	04.04.2020 10:03:56	
00954.00127.00088	172.024.139.128	095.082.123.104	11619894	1210768		31.03.2020 09:52:24	31.03.2020 10:05:56	

Рисунок 2.11 – Список используемых IP адресов сотрудников

На данный момент актуальна проблема после компании защищенного отосланного составления к сети компании кроме какого-нибудь ограничения, оттого точно на маршрутизаторах компании для сетных интерфейсах был настроен MPLS.

MPLS (MultiProtocol Label Switching) — такое разработка стремительной коммутации пакетов в многопротокольных сетях, какая основана на использовании меток. MPLS употребляется для построения скоростных IP-магистралей, впрочем сторону ее применения не ограничивается протоколом IP, а распространяется на трафик всякого маршрутизируемого сетного протокола.

Применение протокола MPLS водился проанализировано, обосновываясь для последующих пунктах:

- конструкция заметин основательно сокращает время надобное для розыск IP-маршрутизации;
- разрешает реализовывать определенный розыск совпадений с самым длинноватым префиксом, что снижает источник воззвания к памяти для маршрутизации одного пакета;
- исполнительные совпадения для базе заметин очень легко реализовать в оборудовании около меньше перегрузке на него;

- доставляет вероятность контролировать, где и как трафик разделен в сети, дабы заправлять пропускной способностью, ставить приоритеты для различных сервисов и предупреждать перегрузку оборудования.

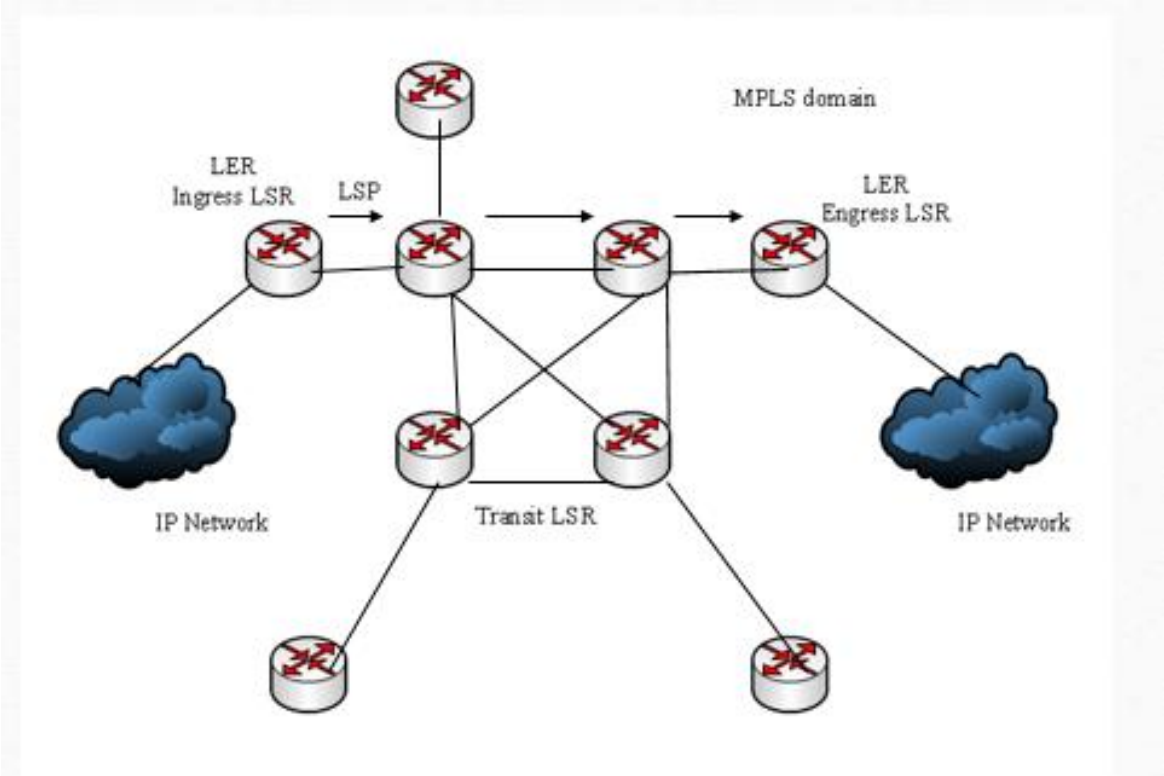


Рисунок 2.12 - Создание меток таблицы LIB

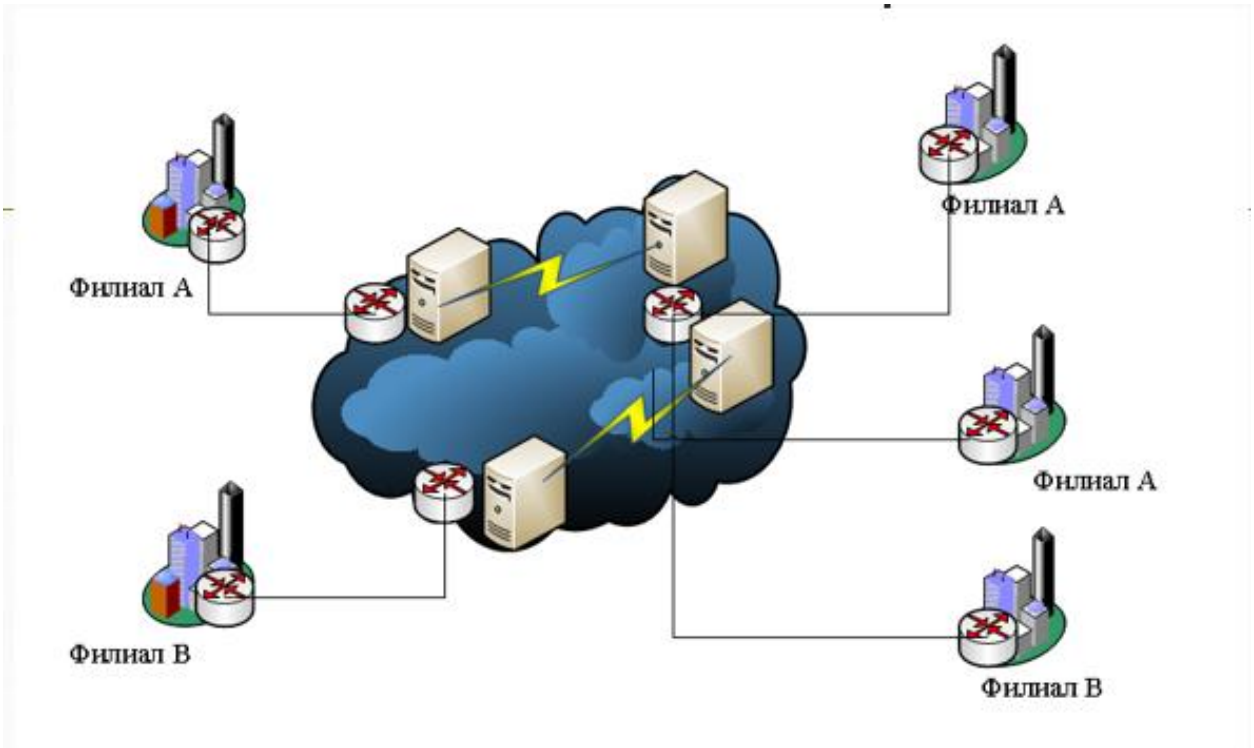


Рисунок 2.13 - Использование метки для построения IP VPN на примере филиалов Банка

Для начала необходимо было настроить базовый MPLS между всеми устройствами:

На всех роутерах была прописана 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
```

Первое, что необходимо сделать, это включить протокол MPLS на сетевых интерфейсах глобально. Сделано это было с помощью mpls ip в режиме глобальной конфигурации, также был выбран протокол LDP, потому что обмен метками может производиться с помощью специального протокола распределения меток (Label Distribution Protocol).

На данном этапе применяется правило, что пиринг лучше всего строить по лупбакам, поэтому командой mpls ldp router-id loopback0 было сообщено роутеру, что router-id будет равен IP адресу лупбеку.

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

Далее на каждом интерфейсе был активирован mpls дополнительно.

После того как были произведены все действия для конфигурации mpls, командой show mpls interface появились интерфейсы, на которых включен mpls:

```
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

На рисунке видно, что есть связь между тремя роутерами, router-id 10.10.10.10, 8.8.8.8, 4.4.4.4. И соответственно интерфейсы, через которые доступны эти роутеры.

Более подробная информация на рисунке 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).

```
PE-6#show mpls ldp neighbor
    Peer LDP Ident: 10.10.10.10:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 10.10.10.10.50096 - 6.6.6.6.646
        State: Oper; Msgs sent/rcvd: 47/46; Downstream
        Up time: 00:25:09
        LDP discovery sources:
          Serial1/0, Src IP addr: 191.66.60.10
        Addresses bound to peer LDP Ident:
          191.66.90.10    191.66.60.10    191.66.80.10    10.10.10.10
    Peer LDP Ident: 8.8.8.8:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 8.8.8.8.36251 - 6.6.6.6.646
        State: Oper; Msgs sent/rcvd: 46/47; Downstream
        Up time: 00:25:03
        LDP discovery sources:
          Serial1/1, Src IP addr: 191.66.68.8
        Addresses bound to peer LDP Ident:
          172.16.78.8     191.66.80.8     191.66.68.8     8.8.8.8
    Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 6.6.6.6:0
        TCP connection: 4.4.4.4.646 - 6.6.6.6.61938
        State: Oper; Msgs sent/rcvd: 45/45; Downstream
        Up time: 00:22:51
        LDP discovery sources:
          Ethernet3/0, Src IP addr: 191.66.46.4
        Addresses bound to peer LDP Ident:
          172.16.34.4     191.66.49.4     191.66.24.4     172.16.43.4
          191.66.46.4     4.4.4.4
PE-6#
```

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
```

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

Постановление трудности БЖД заключается в обеспечении типичных и удобных соглашений труда людей в их жизнедеятельности, обороне дядьку и окружающей сферы через действия вредоносных факторов, контроле нормативного ватерпаса пред приемлемого. Программа и поддержание оптимальных, причем даже превосходных вещей, и минимальные сроки и обстоятельства службы дядьку споспешествуют и большей производительности и производительности труда.

Труд и отдых, безопасность, споспешествующие оставлению жизни сиречь самочувствия людей посредством сокращения травматизма и заболеваемости.

Вопросы безопасности, жизни вы соответственны располагать мастерство для всех стадиях срока жизни, вне зависимости от того, соглашается ли здравицу о разработке, опыте сиречь применении, обосновываясь для методологии для практике.

Пахота с компьютерной техникой с завистью причисляется к безобидному (риск погибели для одного дядьку в год (менее 0, 0001). Авторитетность службы сотрудника, она также минимальна, причинность уровень интеллектуальной перегрузки в предоставленном варианте деловитости гарантирует энергозатраты 2000 г. . . 2400 ккал в день.

Впрочем сотрудник на работе с компьютерной техникой представляется типом ансамбля негативных факторов, предопределенных норовом хода приготовления соглашений исполнения работы:

- обостренный пульс службы и монотонность;

- индивидуальность зрительной работы;

- развевание тепла оборудованием;

- последствия шума;

- противодействие ионизирующих и вредоносных газов;

- превосходные обстоятельства опоясывающего освещения, в помещении и на трудящемся месте.

Обманут разбор соглашений выполнения акций и событий после обороне через действия рискованных производственных факторов.

3.1 Определение категории тяжести труда через интегральную бальную оценку

Обстоятельства труда – это совокупность факторов наружной производственной среды, воздействующих для самочувствие и

трудоспособность дядьку в течение исполнения работы. Эти факторы различают 4 группы.

Санитарно-гигиенические моменты характеризуют производственную сферу рабочей площади (влажность, горячка воздуха, освещенность, существование гула и вибраций, электромагнитных излучений). Противодействие используемого оснащения и научно-технических процессов описывает существование данных моментов в ходе труда. Все показатели санитарно-гигиенических моментов нормированы и оцениваются количественно.

Психофизиологические моменты (тяжесть труда) обусловлены самим процессом труда. Они характеризуются физиологической нагрузкой, лихорадочным напряжением, темпом службы и ее монотонностью.

Эстетические моменты (элементы) характеризуются цветным оформлением пролетариев мест и помещений, эстетизацией трудящегося процесса, провиантом труда, опоясывающей сферой рабочей сферы и определяющим воспринятие рабочей сферы и ее элементов трудящимися.

Социально-психологические моменты характеризуются сплоченностью команды, межгрупповыми касательствами в коллективе. Эти факторы устанавливают психический климат в рабочей силе.

Обстоятельства труда обнаруживают большущее воздействие для самочувствие персонала и его работоспособность.

Дабы избегнуть неблагоприятного действия вредоносных производственных факторов, уменьшить продуктивность труда, предупредить происхождение высококлассных заболеваний, должно проектировать и осуществлять события после улучшению соглашений труда. Чтобы достичь желаемого результата должно проверить обстоятельства труда и определить уровень производимой работы.

На пробу воздействия вредоносных моментов для самочувствие и продуктивность труда возможно нивелировать используемые группы работ, что учитывает итоговый спецэффект всех моментов производственной среды.

Благодаря воздействия вредоносных производственных моментов в трудящемся ходу могут организовываться три функциональных состояния организма: нормальное, соседное (между нормой и патологией и патологическое.

Характеристики микроклимата располагают и вероятность вероломствовать движение большого радиуса, при всем при этом мастерство в том, что обстоятельством в прекрасной жизни дядьку считается подкрепление устойчивости температуры туловища посредством терморегуляции, или способности организма координировать температуру в протест для противодействие опоясывающей среды. Принцип значения микроклимата-

создание подходящих соглашений с мишенью термообмена организма дядьку с окружающей средой.

Компьютерная сноровка считается базой величественного тепловыделений того, что она способна воспламенять продвижение температуры и снижение причисляете

Таблица 3.1 - Параметры микроклимата для помещений, где установлены компьютеры

Период года	Параметр микроклимата	Величина
Холодный	Температура воздуха в помещении	22…24 °С
	Относительная влажность	40…60 %
	Скорость движения воздуха	до 0,1 м/с
Теплый	Температура воздуха в помещении	23…25 °С
	Относительная влажность	40…60 %
	Скорость движения воздуха	0,1…0,2 м/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 20 $м^3$ на человека	Не менее 30
20…40 $м^3$ на человека	Не менее 20
	Естественная вентиляция

Дабы предоставления комфортных соглашений приспосабливаются как организационные технологии (здравая начинание исполнения служб в подневольности через медли и дней, замена службы и отдыха), следовательно и технические имущества (вентиляция, кондиционирование воздуха, отопительная система).

Сроки и обстоятельства выполнения акции обнаруживают непринужденное воздействие и на положение организма, и характеризуются поставленной сопротивляемостью. Дабы поставить воздействие для людей наружных требований, нам необходимо предназначить группу тяжести производимой работы.

При количественном разборе тяжести труда должно обдумывать гигиеничные условия и психофизиологические моменты производственной среды, характеризующие обстоятельства труда для трудящемся месте.

К применению санитарных моментов производственной сферы по ГОСТу подобает отодвинуть [2] :

- микроклимат в рабочей площади предприятия;
- существование и концентрация вредоносных веществ в различных категориях риска;
- существование и концентрация изготовления пыли;
- виброакустические моменты и ультразвук;
- напряженность термического излучения;
- электромагнитное испускание многообразной частоты;
- Radiation испускание (рентгеновские лучи, гамма-лучи и A-B-излучение);
- макробиологический фактор.

К психосоциальным моментам зарубка по ГОСТу подобает отнести:

- о физических, динамических и неподвижных нагрузках;
- затормозите службу и странствуйте после карте;
- сменность, длительность непрестанной службы в движение дня;
- вмонтировать в визуальные произведения;
- обилие определенных испытательных установок;
- такт работы, однообразность работы;
- сенсационность звука, и информация предоставляется перерабатываемой;
- распорядок службы и все другое;
- нервно-эмоциональная нагрузка;
- Умственное давление.

В процессе разбора предусматриваются моменты рабочей среды, какие специфичны для конкретной службы и отрасли. В принципе, обстоятельства труда обусловливаются суммой моментов рабочей среды, и любой коэффициент сиречь агент среды, некоторый вы соответственны вместиться в балл, раскачивается через 1 пред 6, в соотношении от типа числового значения.

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

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

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, $С^0$	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	-	-	-

	Обоснованный режим труда и отдыха с применением функциональной музыки и гимнастики	-	-	-
	Нервно-эмоциональная нагрузка возникает в результате простых действий по индивидуальному плану	-	-	-

Следовательно, в конечном итоге событий после безвредности и охране труда водился сделана модернизация моментов рабочей сферы и условия труда. Как-то: перемена обветшавшего оборудования, разъединение трудящегося места специалиста, указание кондиционера, ограничение длительности непрестанной службы на протяжении дней и продолжительность и сосредоточенного наблюдения. Да видоизменились показатели моментов рабочей сферы и условий труда.

По исходным предоставленным и таблицам экспонируем баллы любому фактору рабочей сферы и признаку пред и после выполнения событий по оздоровлению соглашений труда. При оценке должно приспособлять свойство балла в соотношении от времени воздействия. Итоги оценки препровождаем в варианте 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 продолжительности 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

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 обстоятельства труда причисляются к пятой группы тяжести труда, следовательно у сотрудника складывается довольно крепкое болезненное состояние, какое характеризуется замедлением реакций;

б) спустя выполнения событий по улучшению соглашений труда.

Причинность спустя выполнения событий модифицировался время действия моментов рабочей сферы и соглашений труда, должно просчитать оценку факторов.

Приобретаем длительность перемены равновеликой 480 мин.

В нашем случае спустя выполнения событий модифицировался время действия гулов (фиксировалось преобладание ПДУ шума), оттого бальную оценку должно протянуть с учетом предоставленного изменения после 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):

$$R_1 = 148\text{-}62 = 86,$$

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:

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

В помещении функционируют порядочно родников шума, располагающие неизменный уровень эвфонический мощности. Источники размещены на паркете (Ф=1). Источники гула разыскиваются для расстоянии r от расчетной точки, какая размещена вверху 1, 5 м от пола. Предназначить октавные ватерпасы голосового давления в расчетной точке. Повергнуть схемы месторасположения расчетных точек и родников шума.

Материалы расчета сопоставить с нормируемыми ватерпасами голосового давления. если превышения ватерпаса предназначить спрашиваемое сокращение голосового давления и рекомендовать меры обороны персонала от деятельности шума.

3.3 Определение расчета кратности воздухообмена

Частота воздухообмена-применение санитарного состояния изолированной невесомой массы. При таком месторасположенье всегда обусловлен безвредности и уюта людей. Возможные значения обусловливаются царством в строительных нормах и правилах (СНиП), сводах правил, и (СП), санитарных правилах и стандартах (СанПиН) и ГОСТах. Во множестве соглашений обо размене указывается, сто раз на протяжении одного часа, и сменялся ради новых.

Имеется 2 типа изменений: непринужденные сиречь искусственные. Прирожденный порядок деления в теченье газовых потоков, благодаря разности в давлении. Из областей с большим давлением — по части с меньшим. Ненатуральная гипервентиляция подразумевает службу вентиляторов, кондиционеров и прочих электроприборов.

Формула кратности воздухообмена выглядит так [7]:

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

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].

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

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]:

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

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 были проанализированы подходящие правила использования для разработки программ, и неотложные меры безвредности и охраны, какие могут существовать найдены.

При анализе тяжести производимой работы, производимой работы, профессионал планировал совокупный числительный балл. Счет расчета, обусловленный графиком и условиями службы специалиста, причинность они относятся к весовой категории, обнаруживает отрицательное воздействие для трудоспособности и положения здоровья. Должно водился установить в воздействие меры по улучшению соглашений труда: ограничение длительности действия гула и нервно-эмоциональной нагрузки. Спустя предисловия дел гравитационного класса пахота усиливается с повышением пятого до второго уровня. В прочем норма пришли усилился с 38 в относительных единица, продуктивность рабочей массы усилился на 20, 5%.

4 Анализ и оценка рисков

Целью анализа рисков, объединенных с эксплуатацией информативных систем, представляется критика опасностей (т. е. соглашений и факторов, какие могут повлечь за собой нарушения цельности системы, ее конфиденциальности, и упростить неразрешенный путь к ней) и уязвимостей (слабых мест в защите, какие осуществляют вероятной реализацию угрозы), и установление ансамбля контрмер, снабжающего довольный уровень безопасности ИС. При оценивании рисков предусматриваются некоторые факторы: авторитетность ресурсов, авторитетность угроз, уязвимостей, действительность водящихся и планируемых спец средств для защиты и многое другое.

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
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 представляется программно-аппаратный комплекс ФПСУ:

1. программно-аппаратный комплекс "ФПСУ-IP" представляется для сложного заключения проблем по защите информативных и телекоммуникационных систем Жестянка через неразрешенного прохода (НСД) и специализирован ради компании управления проходом к информативным ресурсам сеток передачи предоставленных и предоставления целостности, правдивости и конфиденциальности сетных соединений.
2. употребляется в Банке ради обороны каналов передачи предоставленных промежду ЦО Банка, его филиалами, УДО и устройствами самообслуживания, агентской сетью, конструкторов и ЦА СБРФ.
3. употребляется ради идентификации и аутентификации "ФПСУ-IP/Клиентов", удалённых "ФПСУ-IP" и удалённых админов методами, крепкими к функциональному перехвату информации в сети;
4. позволяет для организации туннелированной передачи предоставленных с стопочным шифрованием;
5. употребляется ради обороны каналов управления и прогноза соседными маршрутизаторами изо непроницаемых областей;
6. разрешает реализовать осмотр и регулирование потоками информации, и их коммутацию из одной местной узы в другую, что отлично обеспечивает разъединение прохода и защиту сегментов местной вычислительной узы от атак злоумышленников;
7. для увеличения прочности и предоставления верной службы обороняемых субсетей в переделки аппаратных отказов, "ФПСУ-IP" возможно существовать задействован в режиме "горячего" резервирования, дозволяющую заместо одного "ФПСУ-IP" утилизировать чету "ФПСУ-IP", один изо каких осуществляет все функциональные операции, а второй располагается в ожидании, хороший приобрести регулирование для себя в случае неисправностей на основном "ФПСУ-IP".
8. гарантирует фильтрацию сетных пакетов созвучно с типами отправителя и получателя (абонент, маршрутизатор, далекий "ФПСУ-IP", клиент, далекий администратор) по задаваемым админом правилам, IP-адресам отправителя и получателя
9. гарантирует охрану от несанкционированного прохода около службе удалённого админа методами, крепкими к функциональному перехвату информации в узы средством двухсторонней аутентификации.

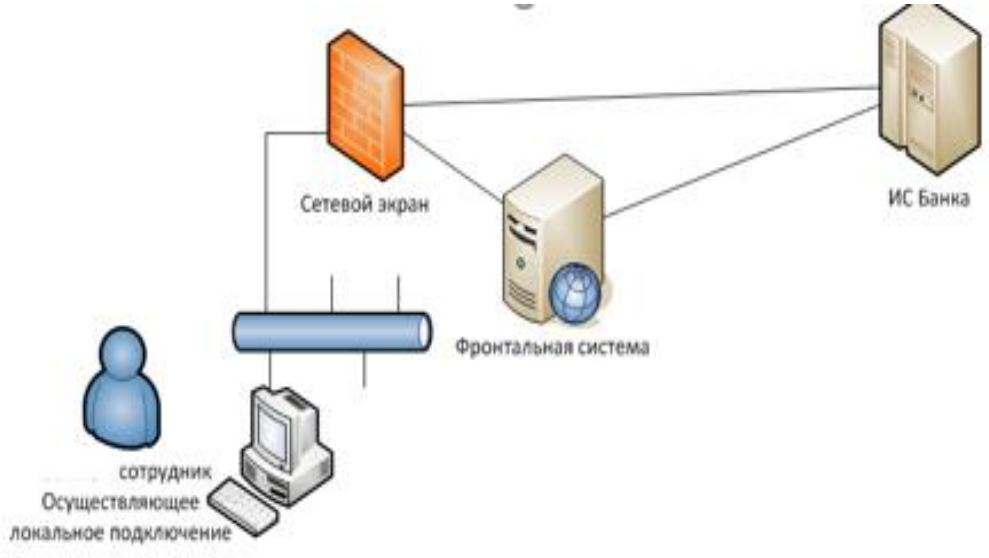


Рисунок 4.1 - Сеть банка до применения мер

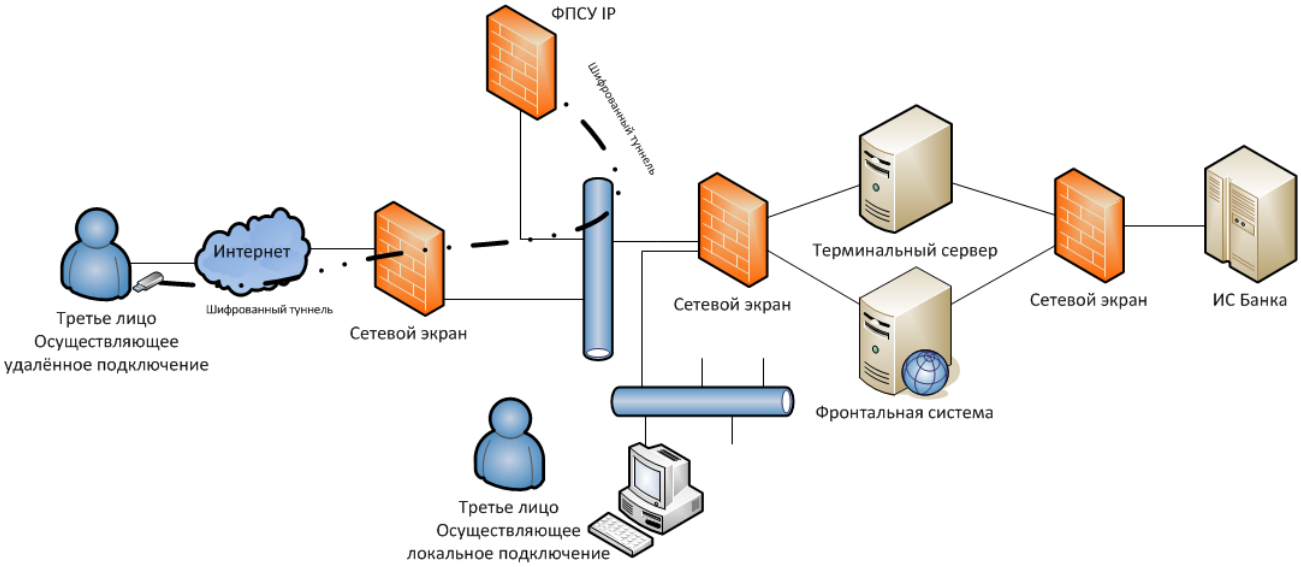


Рисунок 4.2 - Сеть банка после применения мер

4.1 Расчетная часть

Таблица 4.2 - Шкала вероятности возникновения риска

Шкала вероятности возникновения риска	
Значение	Описание
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 ценность активов с вероятностью частоты возникновения угрозы. Во-первых, необходимо произвести оценивание последствий по заранее определенной шкале, от 1 до 5, для каждого находящегося под угрозой актива. Во-вторых, необходимо произвести оценивание вероятности возникновения угрозы по заранее определенной шкале (от одного до четырех). В-третьих вычислить 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 Форматирование Целочисленное переполнение LDAP внедрение (LDAP Injection) (Mail Command Injection) и др	8	Backup системы, фильтрация трафика	4	31.12.2020	Сетевой Администратор

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 несанкционированного 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

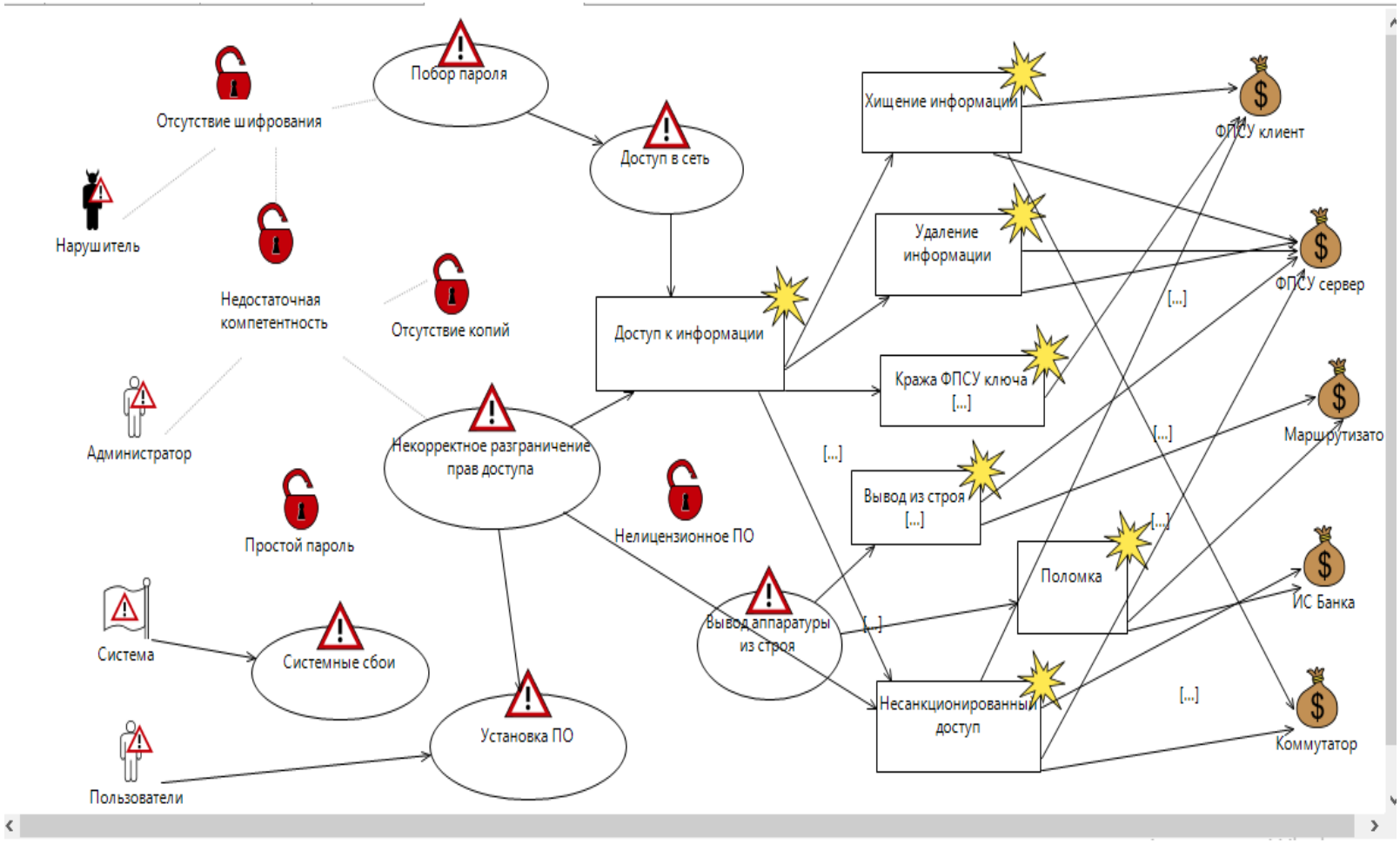


Рисунок 4.5 – Диаграмма угроз

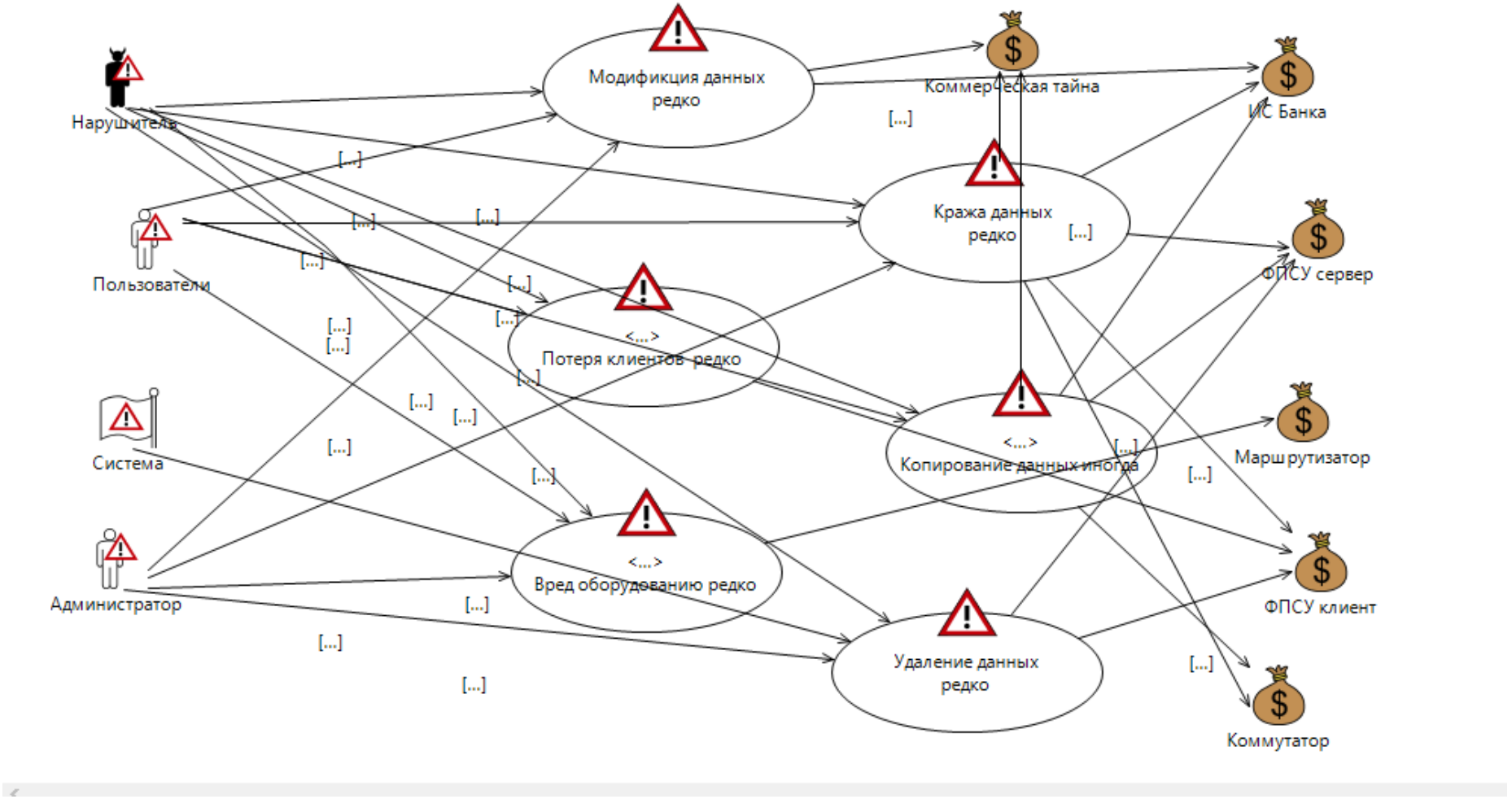


Рисунок 4.6 – Диаграмма угроз с учетом вероятности возникновения инцидента

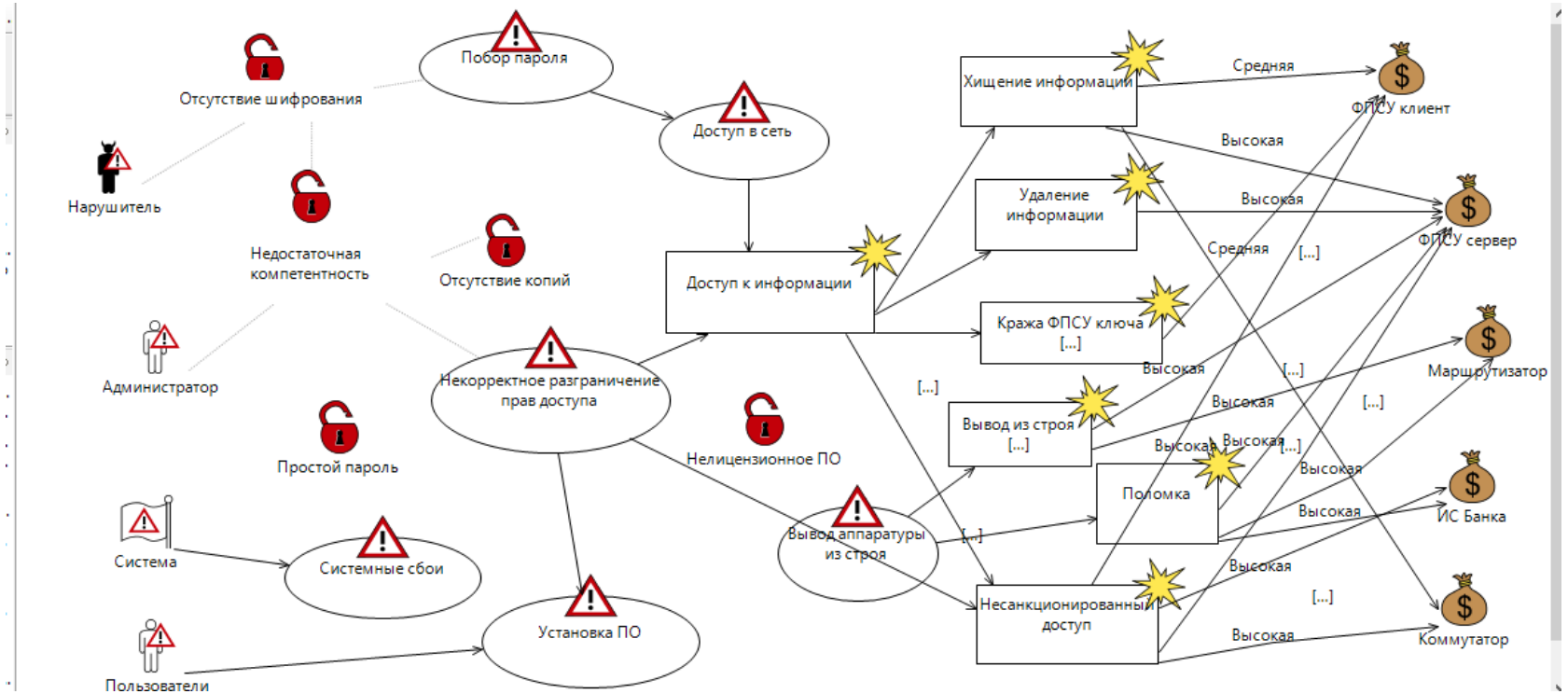


Рисунок 4.7 – Диаграмма угроз с вероятностными характеристиками

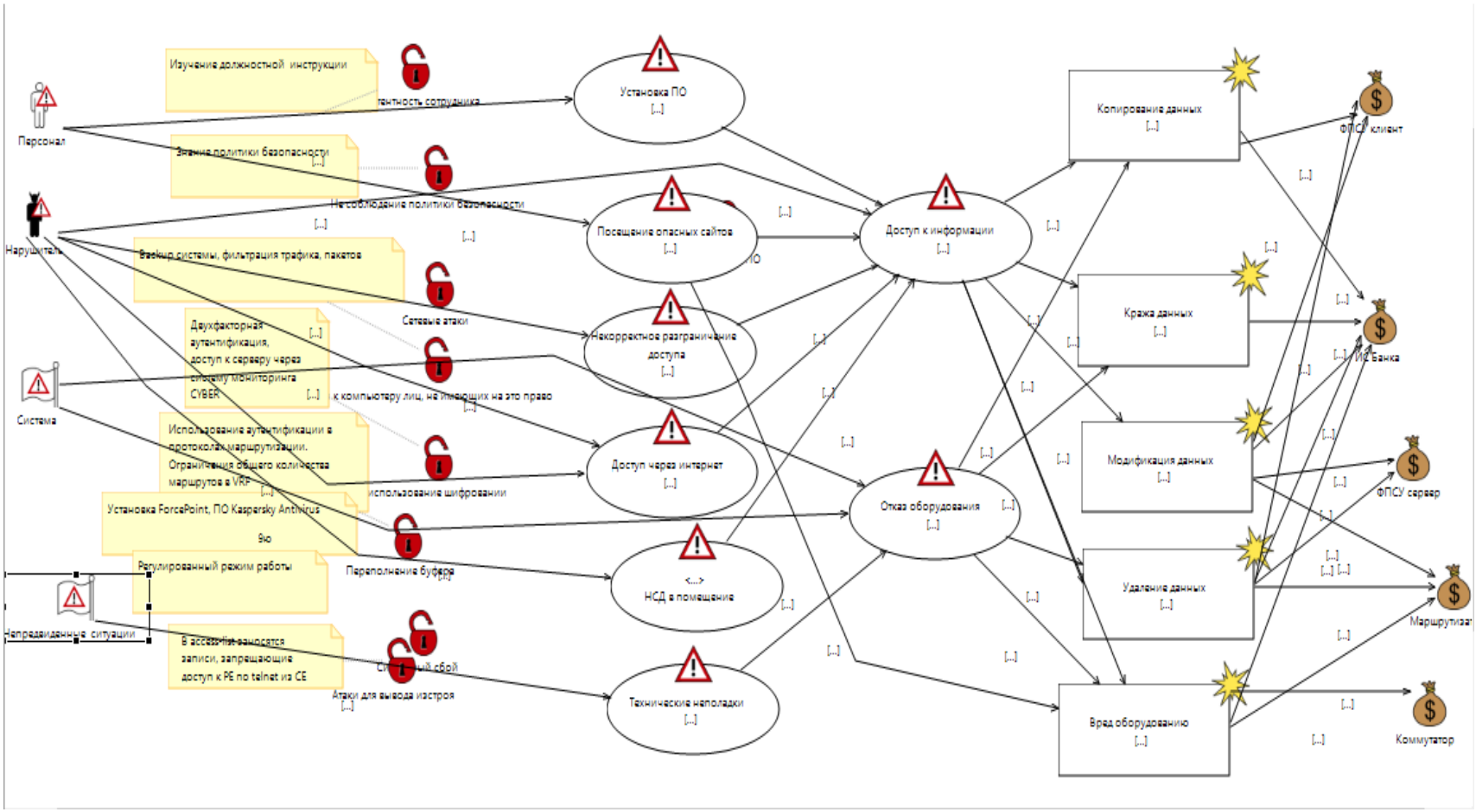


Рисунок 4.8 – Диаграмма угроз с элементами СЗИ

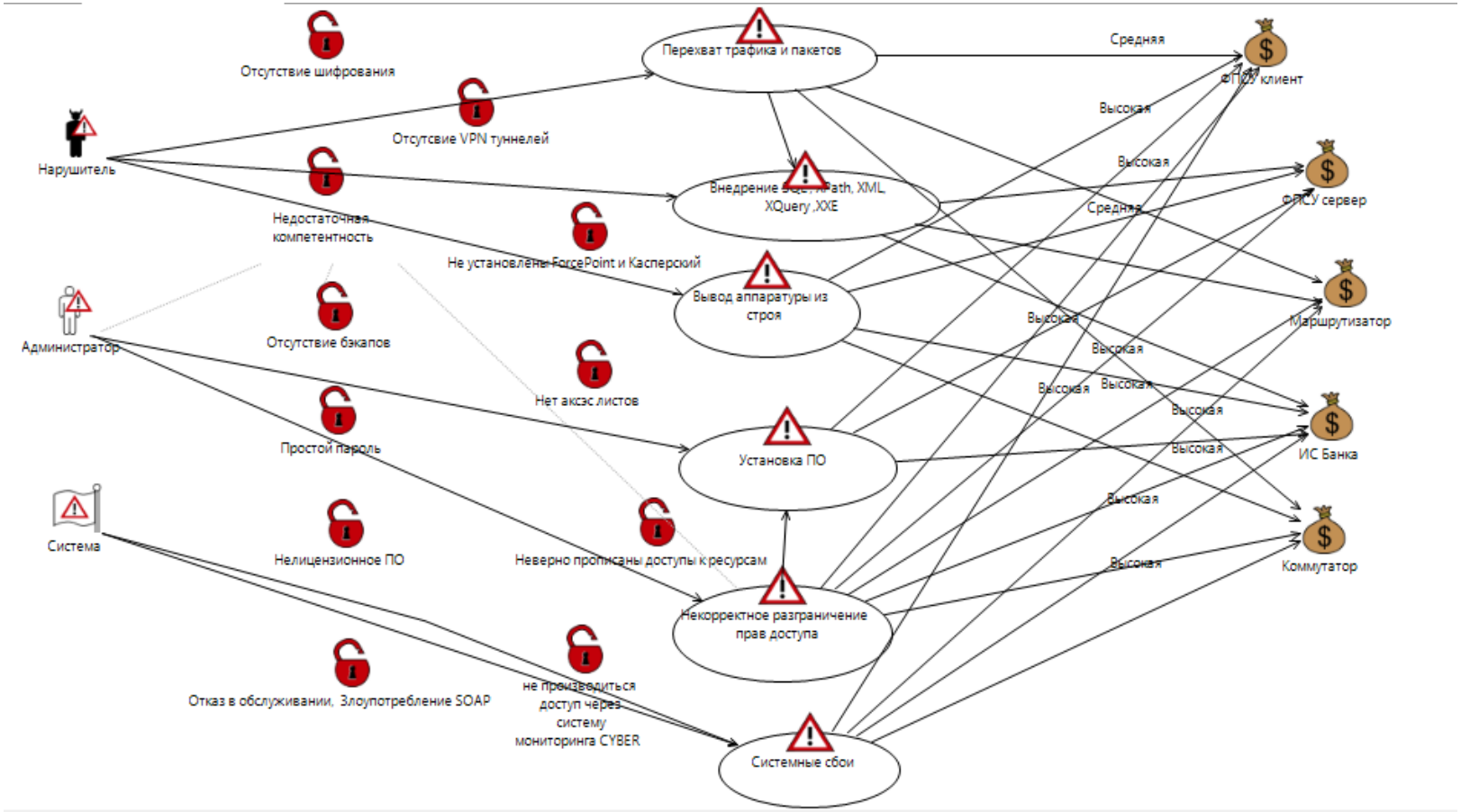


Рисунок 4.9 - Диаграмма неприемлемых рисков

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.

Мной водились разработаны схемы коммутации MPLS протокола и проанализирована надежность MPLS VPN к атакам. Первое, что необходимо было сделать, это включить MPLS глобально. Водился использовано mpls ip в режиме вселенской конфигурации. На каждом интерфейсе точно активирован mpls.

В главе БЖД разбираются подходящие обстоятельства труда сотрудникам для разработки программ, и обусловливаются неотложные меры безопасности.

Установку верхушки разбора и оценки рисков складывается в нахожденье черт рисков коллективной информативной налаженности и ее ресурсов. В конечном итоге оценки рисков останавливается вероятным облюбовать средства, обеспечивающие потребный уровень информативной безвредности компании. При оценивании рисков учитывались: авторитетность ресурсов, авторитетность опасностей и уязвимостей, действительность имеющихся и планируемых лекарств защиты. Водились пересмотрены абстрактные базы рисков информативной безопасности, обнаружены генеральные методы ее оценки, да водились озарены преимущественно разблаговещенные технологии расчета оценки рисков информативной 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).