Федеральное агентство связи
Федеральное государственное бюджетное образовательное учреждение высшего образования «Сибирский государственный университет телекоммуникаций и информатики»
(СибГУТИ)

11.03.02 «Инфокоммуникационные технологии и системы связи»
Профиль «Защищенные сети связи»
№ кода и наименование направления подготовки

ОТЧЕТ

Ознакомительная практика

Выполнил(а):
студент(ка) № группы _____/Фамилия И.О./
дата подпись

Руководитель практики от университета: _____/Фамилия И.О./
должность ОЦЕНКА
дата

Новосибирск 2021

СОДЕРЖАНИЕ

Введение

Прохождение практики является одним из основных этапов подготовки студента. Она позволяет углубить полученные в ходе обучения теоретические знания.

Цель практики заключается в закреплении теории и приобретении практических навыков и опыта для дальнейшего обучения, будущей практической деятельности, а также овладения элементами делового общения в трудовом коллективе.

Под защитой информации в компьютерной системе понимается принятие мер, направленных на поддержание безопасности хранящейся и обрабатываемой информации, а также ассоциированных с ней компьютерных ресурсов. Принимаемые меры основаны на использовании средств и методов защиты. Соответственно, система защиты информации или, как ее еще называют, система информационной безопасности определяется как организационная совокупность всех мер, методов и средств, предусмотренных для поддержания информационных ресурсов в безопасном состоянии, т.е. в состоянии, которое соответствует установленному статусу их хранения, обработки и использования. Задача построения системы информационно-компьютерной безопасности является противоречивой и сложной. Противоречивый характер данной задачи состоит в том, что система информационно-компьютерной безопасности должна удовлетворять двум группам требований: – требованиям по надежной защите информационных ресурсов; – требованиям по удобству использования компьютерной системы.

Чтобы надежно защитить информационные ресурсы, система информационно-компьютерной безопасности должна обеспечивать защиту:

– компьютерных ресурсов от несанкционированных лиц;

– компьютерных ресурсов от санкционированных пользователей при выполнении ими несанкционированных или некорректных действий;

– санкционированных пользователей друг от друга при выполнении ими несанкционированных или некорректных действий;

– каждого санкционированного пользователя от себя самого (от его некорректных действий);

– процесса обработки данных от отказов (нарушений работоспособности).

В ходе учебной практики рассмотрены вопросы деятельности предприятия и степень защищенности его ресурсов.

1. Общая характеристика организации

АО «Дальневосточная генерирующая компания» (АО «ДГК») — российская генерирующая энергетическая компания, действующая в Амурской области, Еврейской автономной области, Хабаровском крае, Приморском крае и южной части Якутии. Штаб-квартира — в городе Хабаровске.

АО «Дальневосточная генерирующая компания» было создано 19 декабря 2005 года в рамках реформы РАО «ЕЭС России». В 2006—2007 годах в собственность компании были переданы электростанции, котельные и тепловые сети ОАО «Хабаровскэнерго», ЗАО «ЛуТЭК», ОАО «Дальэнерго», ОАО «Южное Якутскэнерго» и ОАО «Амурэнерго». С 2011 года компания входит в группу РусГидро.

Дальневосточная генерирующая компания обеспечивает производство электроэнергии в регионах, входящих в Единую энергосистему Востока, а также обеспечивает теплоснабжение (как в части производства, так и сбыта тепла). В Хабаровском крае является доминирующей энергокомпанией.

Основными видами деятельности АО «Дальневосточная генерирующая компания» являются:

- производство тепловой и электрической энергии;
- транспортировка с наименьшими потерями тепловой энергии потребителям;
- распределение теплоэнергии между потребителями;
- обеспечение безаварийной передачи теплоэнергии;
- обеспечение тепловой энергией Дальневосточного региона, при которой возникновение и развитие кризисных ситуаций региона сведено к нулю;
- поставка (продажа) электрической и тепловой энергии по установленным тарифам в соответствии с диспетчерскими графиками электрических и тепловых нагрузок;
- организация энергосберегающих режимов работы оборудования электростанций, соблюдение режимов поставки энергии в соответствии с договорами;
- реализация (продажа) тепловой энергии на розничных рынках тепловой энергии потребителям (в том числе гражданам);
- обеспечение энергоснабжения потребителей, подключенных к электрическим и тепловым сетям Общества, в соответствии с заключенными договорами;
- добыча и реализация угля.

Структура АО «ДГК» представлена на рисунке 1.1.

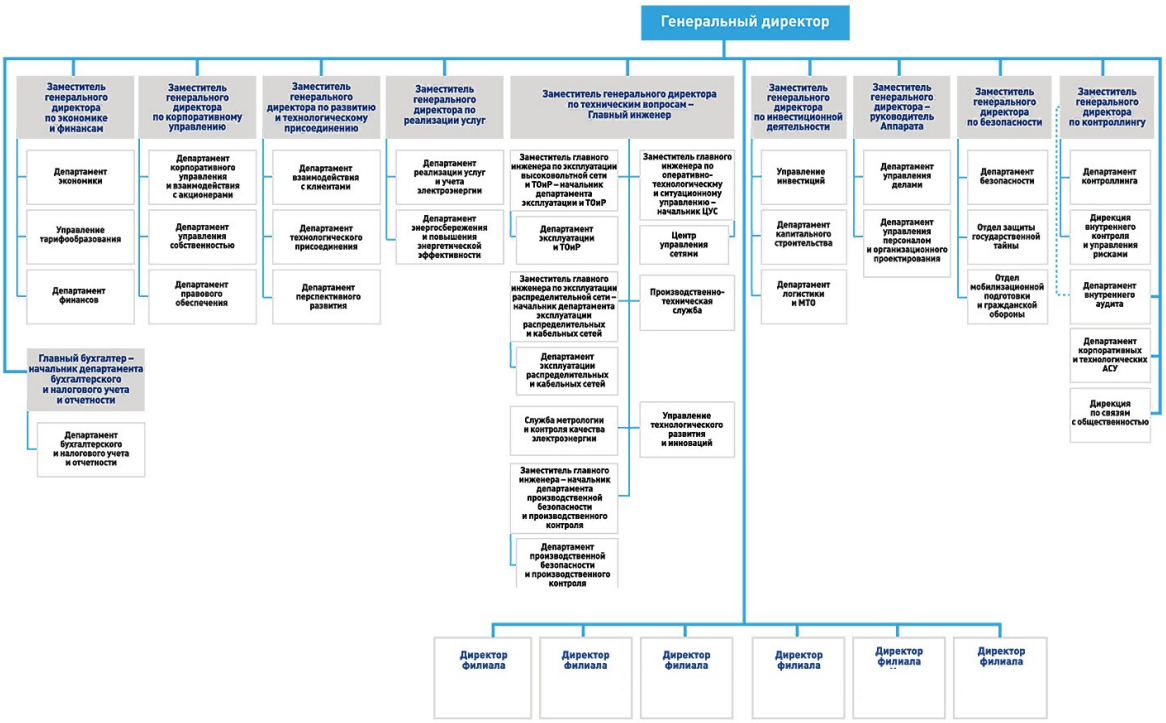

Рисунок 1.1 – Структура АО «Дальневосточная генерирующая компания»

На рисунке 1.2 представлена существующая корпоративная сеть АО «Дальневосточная генерирующая компания» в г. Хабаровск.

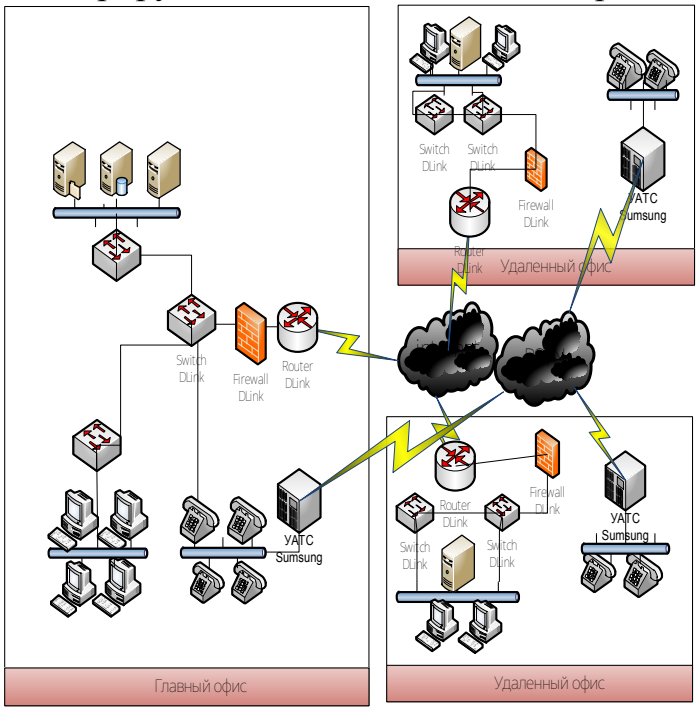

Рисунок 1.2 - Существующая корпоративная сеть АО «Дальневосточная генерирующая компания» в г. Хабаровск

Корпоративная сеть компании обеспечивает предоставление услуг по передаче трафика данных между центральным офисом, и филиалами на базе сервисов протоколов IP. Объединение различных подсетей корпоративных клиентов происходит посредством передачи IP-пакетов через сеть оператора.

Услуги корпоративной IP-сети предоставляют следующие возможности:

- передачи трафика между одиночными абонентами, а также между территориально-распределенными элементами сетей корпоративных клиентов на третьем уровне модели OSI, на уровне IP-пакетов;
- возможности управления качеством обслуживания (QoS) на уровне IP-пакетов и предоставление разных уровней сервиса в зависимости от потребностей клиента;
- маршрутизации трафика клиентов средствами сети оператора;
- предоставления клиентам согласованного пространства IP-адресов.

В структуре корпоративной распределенной сети при создании учтены все три уровня: уровень доступа, уровень концентрации и уровень сервисов.

Уровень доступа основывается на использовании коммутатора доступа (КД), который является узлом доступа городской операторской сети. Коммутаторы доступа располагаются во всех офисах компании и обеспечивают доступ клиентов к тем услугам, которые предоставляет городская сеть оператора.

В качестве коммутаторов доступа используются DES-1100-24: настраиваемый L2 коммутатор с 24 портами 10/100Base-TX. Серия коммутаторов DES-1100 EasySmart объединяют полный набор настраиваемых функций, обеспечивающих лучшую производительность и масштабируемость. Линейка коммутаторов EasySmart представлена моделями DES-1100-16 с 16 портами 10/100 Мбит/с, DES-1100-24 с 24 портами 10/100 Мбит/с и DES-1100-26 с 24 портами 10/100 Мбит/с и 2 гигабитными комбо-портами. Коммутаторы помогают пользователям легко и быстро развернуть сеть благодаря простому управлению с помощью утилиты SmartConsole или через Web-интерфейс. Коммутатор серии DES-1100 представляет собой законченное и недорогое решение для сетей малого и среднего бизнеса (SMB). DES-1100 является подходящим решением для развертывания сетей предприятий, например, для филиалов и помещений для деловых встреч, где требуется простое управление.

Уровень концентрации содержит узловые коммутаторы (УК), являющиеся концентрирующими узлами городской операторской сети. УК обеспечивают функции агрегирование трафика коммутатора доступа и передачу агрегированных потоков до других узловых коммутаторов сети оператора. В каждом здании компании установлено по одному узловому коммутатору.

В качестве узловых коммутаторов на сети установлены коммутаторы третьего уровня серии DES-3810-28, входящие в семейство D-Link xStack, обеспечивают высокую производительность, широкие функциональные

возможности, в том числе и уровня 3. Коммутатор DES-3810-28 оснащен 24 портами 10/100 Мбит/с Fast Ethernet и 4 комбо-портами 1000Base-T/SFP Gigabit Ethernet. Порты Fast Ethernet обеспечивают подключение к другим коммутаторам LAN. Комбо-порты обеспечивают гибкое подключение к магистрали сети и центральным коммутаторам.

Функциональность операторской сети в части организации предоставления услуг, а так же управления услугами, и управления стыками с внешними сетями и информационными системами выполняется за счет функциональности оборудования КД, УК и рабочих станций системы управления сети оператора.

Управление активным сетевым оборудованием и сервисами производится средствами специализированного программного обеспечения, которое установлено на рабочих станциях системы управления сети оператора.

Межсетевой экран установлен в каждом офисе компании и реализован на оборудовании DFL-870 (D-Link). DFL-870 представляет собой высокопроизводительное решение, обеспечивающее всестороннюю защиту сетей предприятий от разнообразных угроз, таких как вирусные атаки, несанкционированный доступ и вредоносный трафик. DFL-870 также позволяет решать задачи управления, мониторинга и обслуживания безопасной сетевой инфраструктуры в распределенных корпоративных сетях. Данный межсетевой экран оснащен шестью настраиваемыми портами 10/100/1000 Мбит/с, двумя портами USB 2.0, консольным портом с разъемом mini-USB и выполнен в металлическом корпусе с возможностью установки в 19-дюймовую стойку.

Сеть АО «Дальневосточная генерирующая компания» в г. Хабаровск расположена в нескольких зданиях: 4-этажном здании (здание А); 3-этажном здании (здание В) и 2-этажном здании (здание С). Подразделения, а следовательно и рабочие группы, в здании А расположены следующим образом:

1 этаж. Подразделения:

- Руководство;
- Департамент корпоративного управления;
- Департамент управления собственностью;
- Департамент правового обеспечения;
- Департамент взаимодействия с клиентами;
- Серверная;
- Узел связи.

2 этаж. Подразделения:

- Департамент технологического присоединения;
- Департамент перспективного развития;
- Департамент реализации услуг и учета электроэнергии;
- Департамент энергосбережения и повышения энергетической эффективности;

3 этаж. Подразделения:

- Департамент эксплуатации и ТОиР;
- Департамент эксплуатации распределительных и кабельных сетей;
- Служба метрологии;
- Управление технологического развития и инноваций;
- Департамент производственной безопасности и производственного контроля;

4 этаж. Подразделения:

- Управление инвестиций;
- Департамент капитального строительства;
- Департамент логистики и МТО;
- Департамент управления делами.

Всего в здании расположено 35 рабочих места и сформировано 19 рабочих группы в здании.

Количество рабочих мест на одном этаже: 1 этаж – 12 рабочих мест; 2 этаж – 8 рабочих мест; 3 этаж – 10 рабочих мест; 4 этаж – 5 рабочих мест.

Количество рабочих мест в одной рабочей группе: 2 или 1

Количество ПК – по числу рабочих мест – 35 шт.

Количество телефонов: по 1 ТА и 1 IP в каждой рабочей группе – 23 ТА и 25 IP и 3 видеотерминала для рабочих групп.

Общие серверы, расположенные в здании А: File server; E-mail server; FTP-server.

Серверы рабочих групп в здании А: SQL Server; FTP Server; Small office; Database server. Всего в здании А расположен 79 серверов.

Департамент безопасности расположен в 3-х этажном здании В. Всего в здании расположено 8 рабочих мест и сформировано 3 рабочих группы.

Количество рабочих мест на одном этаже: 1 этаж – 4 чел; 2 этаж – 2 чел; 3 этаж – 2 чел.

Количество ПК – по числу рабочих мест – 8 шт. Количество телефонов: 5 ТА и 3 IP.

Общие серверы, расположенные в здании В: File server; E-mail server;

Серверы рабочих групп в здании В: SQL Server; FTP Server; Small office; Database server. Всего в здании В расположено 14 серверов.

Департамент по контроллингу располагается в 2-х этажном здании С. В здании расположено 5 рабочих мест и сформировано 2 рабочих групп: по 5 ПК, 3 ТА и 1 IP-телефон.

В настоящее время в каждом здании имеются небольшие ЛВС, которые объединены в единую корпоративную сеть. Между всеми зданиями А, В и С имеются волоконно-оптические линии связи.

Здание А имеет корпоративный доступ к Интернету по выделенной линии, для чего в серверное помещение проведён оптоволоконный кабель от 2-х Интернет-провайдеров, закреплённый в монтажной панели.

2. Общая защищенность информационных процессов

Рассмотрим достоинства и недостатки программных и аппаратных средств защиты информации.

Законодательные и морально-этические меры определяют правила обращения с информацией и ответственность субъектов информационных отношений за их соблюдение [10].

Законодательные и морально-этические меры противодействия, являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения и НСД к АС и информации. В некоторых случаях они являются единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Организационные меры - это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако, это вовсе не означает, что систему защиты необходимо строить исключительно на их основе [11].

Этим мерам присущи серьезные недостатки, такие как:

- низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);

- дополнительные неудобства, связанные с большим объемом рутинной и формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей системы [10].

Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо перекрыть, всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств (администратора АС, администратора безопасности и т.п.). Вместе с самими средствами защиты эти люди образуют так называемое "ядро безопасности". В этом случае,

стойкость системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер.

Но даже имея совершенные законы и проводя оптимальную кадровую политику, все равно проблему защиты до конца решить не удастся [13].

Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действий, вынуждающих его нарушить запреты.

Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

Построение системы обеспечения безопасности информации в АС и ее функционирование должны осуществляться в соответствии со следующими основными принципами, представленными в таблице 2.1.

Таблица 2.1 – Основные принципы построения системы безопасности

Принцип	Описание
законность	Предполагает осуществление защитных мероприятий и разработку системы безопасности информации в АС в соответствии с действующим законодательством в области информации, информатизации и защиты информации, других нормативных актов по безопасности, утвержденных органами государственной власти в пределах их компетенции, с применением всех дозволенных методов обнаружения и пресечения правонарушений при работе с информацией.
системность	Системный подход к защите информации в АС предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно значимых для понимания и решения проблемы обеспечения информационной безопасности в АС. При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей, пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.
комплексность	Комплексное использование методов и средств защиты компьютерных систем предполагает согласованное применение разнородных средств при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов. Защита должна строиться эшелонировано. Внешняя защита должна обеспечиваться физическими средствами, организационными, технологическими и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства защиты, реализованные на уровне операционных систем (ОС) СВТ в силу того, что ОС - это та часть компьютерной системы, которая управляет использованием всех ее ресурсов. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.
непрерывность	Защита информации - не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации.

	Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, переопределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных "закладок" и других средств преодоления системы защиты после восстановления ее функционирования.
своевременность	Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите АС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки АС в целом и ее системы защиты информации, в частности. Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.
преемственность и непрерывность совершенствования	Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования АС и ее системы защиты с учетом изменений в методах и средствах перехвата информации и воздействия на компоненты АС, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.
разумная достаточность	Предполагает соответствие уровня затрат на обеспечение безопасности информации ценности информационных ресурсов величине возможного ущерба от их разглашения, утраты, утечки, уничтожения и искажения. Используемые меры и средства обеспечения безопасности информационных ресурсов не должны заметно ухудшать эргономические показатели работы АС, в которой эта информация циркулирует. Излишние меры безопасности, помимо экономической неэффективности, приводят к утомлению и раздражению персонала
персональная ответственность	Предполагает возложение ответственности за обеспечение безопасности информации и системы ее обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.
разделение функций	Принцип Разделения функций, требует, чтобы ни один сотрудник организации не имел полномочий, позволяющих ему единолично осуществлять выполнение критичных операций. Все такие операции должны быть разделены на части, и их выполнение должно быть поручено различным сотрудникам. Кроме того, необходимо предпринимать специальные меры по недопущения сговора и разграничению ответственности между этими сотрудниками.
минимизация полномочий	Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью. Доступ к информации должен предоставляться только в том случае и объеме, в каком это необходимо сотруднику для выполнения его должностных обязанностей.
взаимодействие и сотрудничество	Предполагает создание благоприятной атмосферы в коллективах подразделении. В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений обеспечения безопасности информации.
гибкость системы защиты	Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования.
открытость алгоритмов и механизмов защиты	Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Это однако не означает, что информация о конкретной системе защиты должна быть общедоступна.

простота применения средств защиты	Механизмы зашиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).
научная обоснованность и техническая реализуемость	Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности информации.
специализация и профессионализм	Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информационных ресурсов, имеющих опыт практической работы и государственные лицензии на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными сотрудниками (специалистами подразделений обеспечения безопасности информации).
взаимодействие и координация	Предполагают осуществление мер обеспечения безопасности информации на основе взаимодействия всех заинтересованных министерств и ведомств, предприятий и организаций при разработке и функционировании АС и ее системы защиты информации, подразделений и специалистов органов МВД специализированных предприятий и организаций в области защиты информации, привлеченных для разработки системы защиты информации в АС, координации их усилий для достижения поставленных целей Гостехкомиссией России (на этапе разработки и внедрения АС) и подразделениями безопасности органов МВД (на этапе функционирования системы).
обязательность контроля	Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности информации на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств. Контроль за деятельностью любого пользователя, каждого средства зашиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

Проанализировав информационную безопасность предприятия можно сделать вывод, что в информационной безопасности есть недостатки [15]:

- отсутствие паролей доступа в систему;
- отсутствует дополнительная защита файлов и информации (отсутствует элементарный запрос пароля при открытии или изменении информации в файлах, не говоря уже о средствах шифрования данных);
- нерегулярное обновление баз программы антивируса и сканирование рабочих станций;
- большое количество документов на бумажных носителях в основном лежат в папках (иногда и без них) на рабочем столе сотрудника, что позволяет злоумышленникам без труда воспользоваться данного рода информациях в своих целях;
- не производится регулярное обсуждение вопросов информационной безопасности на предприятии и возникающих проблем в этой области;
- не организована регулярная проверка работоспособности информационных систем предприятия, отладка производится только лишь в том случае, когда они выходят из строя.

3. Состояние организационно-сопроводительных документов

Сотрудники должны соблюдать меры по обеспечению информационной безопасности, а именно:

По возможности не допускать нахождение посторонних лиц в помещениях, в которых ведутся работы с секретной и конфиденциальной информацией. Если же посторонние лица все же были допущены (уборщицы, электрики, и другие сотрудники, не относящиеся к данному предприятию, а так же сотрудники, не имеющие соответствующего уровня доступа), то следует следить за ними, во избежание утечки информации.

Сотрудники не должны самостоятельно устанавливать либо изменять параметры установленного программного обеспечения.

Интернет должен использоваться только для работы.

На предприятии реализованы дополнительные сопроводительные документы, включающие журналы доступа в серверную комнату, журнал тестирования средств информационной защиты, форму на согласие обработки персональных данных как для клиентов, так и для сотрудников организации.

4. Разработка модели нарушителя

Модель угроз является методическим документом, который предназначен для работников АО «Дальневосточная генерирующая компания» в г. Хабаровске и используется при создании ИС, обрабатывающей защищаемую информацию, выборе технических и программных средств защиты информации, проведении работ по технической защите информации.

Модель угроз предназначена для решения следующих задач:

- анализа защищенности информационной системы (ИС) от угроз безопасности защищаемой информации (ЗИ) в ходе организации и выполнения работ по обеспечению безопасности информации и дальнейшего функционирования ИС;
- разработки системы защиты информации, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты информации, предусмотренных для соответствующего класса ИС;
- проведения мероприятий, направленных на предотвращение НСД к защищаемой информации и/или передачи ее лицам, не имеющим права доступа к такой информации;
- недопущения воздействия на технические и программные средства ИС, в результате которого может быть нарушено их функционирование;
- контроля за обеспечением уровня защищенности информации.

Угрозы безопасности информации ИС, описанные в модели угроз, могут уточняться и дополняться по мере выявления новых источников угроз, развития средств и способов реализации угроз безопасности, изменения требований законодательства в области защиты информации.

Кроме того, модель угроз может быть пересмотрена по решению руководства АО «Дальневосточная генерирующая компания» в г. Хабаровске или рекомендации уполномоченных органов государственной власти на основе проводимых мероприятий по контролю выполнения требований по обеспечению информационной безопасности. [12], [14], [15].

Настоящая модель угроз разработана в соответствии с требованиями федерального законодательства и федеральных органов государственной власти:

- Методика ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15.02.2008;
- Методика определения актуальных угроз безопасности ПДН утв. ФСТЭК РФ 14.02.2008;
- Федеральный закон РФ «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ;

- Федеральный закон РФ «О персональных данных» от 27.07.2006 г. № 152-ФЗ;

- Федеральный закон РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. № 149-ФЗ;

- «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены руководством 8 Центра ФСБ России, 21.02.2008 г. № 149/54-144);

- Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требованиям к средствам удостоверяющего центра».

Состав технических средств и программного обеспечения представлен в таблице 4.1.

Таблица 4.1 - Состав технических средств и программного обеспечения

№ п.п	Наименование
Компонент файловый сервер	
1	Технические средства (ТС)
1.1	Файловый сервер
2	Программное обеспечение (ПО)
2.1	Утилита управления СУБД «SQL Server Management Studio Express»
2.2	Операционная система (ОС) «MicrosoftWindowsServer» со всеми компонентами
2.3	Программный комплекс защиты КИ SecretDiskServer NG 3.8
2.4	СУБД «MS SQL Server 2005 Express»
2.5	Антивирусное СЗИ «Kaspersky Endpoint Security»
2.6	СЗИ от НСД «Secret Net 7»
2.8	Программа «Adobe Reader»
Компоненты почтовый сервер и Web-сервер	
1	Технические средства (ТС)
1.1	Web-сервер
2	Программное обеспечение (ПО)
2.1	Операционная система «MicrosoftWindowsServer» со

	всеми компонентами
2.2	Программный комплекс защиты КИ SecretDiskServer NG 3.8
2.3	АнтивирусноеСЗИ «Kaspersky Endpoint Security» и «Kaspersky Security Center»
2.4	СЗИ от НСД «Secret Net 7»
2.5	Программа «Adobe Reader»
Компонент АРМ	
1	Технические средства (ТС)
1.1	ПЭВМ (системный блок, монитор, клавиатура, мышь, KVM-переключатель)
2	Программное обеспечение (ПО)
2.1	Операционная система «MicrosoftWindows 10» со всеми компонентами, необходимыми для работы
2.1	Операционная система «MicrosoftWindows 10» со всеми компонентами, необходимыми для работы
2.2	Антивирусное СЗИ «Kaspersky Endpoint Security»
2.3	СЗИ от НСД «Secret Net 7»
2.4	Пакет программ управления МСЭ
2.5	СУБД «Microsoft SQL Express 2008»
2.6	Программа «Adobe Reader»
Дополнительные компоненты	
1	Межсетевой экран
2	Коммутатор доступа, узловой коммутатор
3	Источник бесперебойного питания
4	Многофункциональное устройство (МФУ)
5	Съемные носители информации для хранения ключевой информации
6	Съемные носители информации для передачи данных
7	Съемные носители информации для резервного копирования

8	Линии передачи информации между компонентами ИС в границах контролируемой зоны (сетевые кабели)
9	Линии передачи информации (сетевые кабели) между компонентами ИС и КИС, выходящие за границы контролируемой зоны
10	Линии электропитания и заземления
11	

На основе анализа условий создания и использования защищенной информации (ЗИ) определена информация, соответствующая процессам создания и использования ЗИ, которая также может быть объектом угроз [12]:

- ключевая, аутентифицирующая и парольная информация: ключи защиты канала связи, ключи Администраторов/Операторов АРМ для подключения к компонентам серверов, ключи к СЗИ от НСД для доступа к информационным ресурсам, пароли доступа к ключевым носителям (личным идентификаторам) и ключевым контейнерам Администраторов/Операторов АРМ, администратора безопасности;
- криптографически опасная информация (КОИ);
- конфигурационная и управляющая информация: конфигурационные файлы ПО, таблицы маршрутизации, настройки СЗИ;
- информация в электронных журналах регистрации: информация в журналах событий компонентов ОС, информация в журналах средств ФС, информация в журналах СЗИ, информация в журналах СУБД.
- побочные сигналы, которые возникают в процессе функционирования технических средств и в которых полностью или частично отражается защищаемая информация;
- резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов;
- остаточная информация на носителях информации.

Объектами угроз являются: защищаемая информация (таблица 4.2), сопутствующая информация (таблица 4.3), программное обеспечение (таблица 4.4), технические средства (таблица 4.5).

Таблица 4.2 – Защищаемая информация

№ п/п	Защищаемая информация	Форма фиксации	Обозначение
1	Ключи ЭП владельцев сертификатов ключей проверки ЭП	Области оперативной памяти ТС — в процессе генерации ключей ЭП	ЗИ1
		Файлы на съемном ключевом носителе	ЗИ2
2	Ключ ЭПФС	Области оперативной памяти ТС	ЗИ3
		Файлы на съемном ключевом носителе	ЗИ4
3	Персональная и корпоративная информация пользователей ИС, не подлежащая рассылке	Записи БД на жестких дисках ТС	ЗИ5
		Записи БД на съемных носителях резервного копирования	ЗИ6
		Данные в сетевых пакетах	ЗИ7
		Изображение на экране монитора	ЗИ8
4	Сертификаты ключей проверки ЭП пользователя и их статус	Файлы и записи БД на жестких дисках ТС	ЗИ9
		Записи БД на съемных носителях резервного копирования	ЗИ10
		Данные в сетевых пакетах	ЗИ11
		Бумажные документы	ЗИ12
		Изображение на экране монитора	ЗИ13
5	Запросы на получение, аннулирование (отзыв), приостановление и возобновление действия сертификатов пользователя	Файлы и записи БД на жестких дисках ТС	ЗИ14
		Записи БД на съемных носителях резервного копирования	ЗИ15
		Данные в сетевых пакетах	ЗИ16
		Файл на съемном носителе информации	ЗИ17

Таблица 4.3 – Сопутствующая информация

№ п/п	Программное обеспечение		Обозначение
1	Ключевая, аутентифицирующая и парольная информация	Записи БД (реестр ОС) на жестких дисках ТС	СИ1
		Файлы на съемном ключевом носителе	СИ2
2	Криптографическиопасная информация	Области оперативной памяти ТС	СИ3
3	Конфигурационная и управляющая информация	Файлы на жестких дисках (или иных энергонезависимых модулях памяти) ТС	СИ4
		Изображение на экране монитора	СИ5
4	Управляющая информация	Данные в сетевых пакетах	СИ6
5	Информация в электронных журналах регистрации	Файлы и записи БД на жестких дисках (или иных энергонезависимых модулях памяти) ТС	СИ7
		Данные в сетевых пакетах	СИ8
		Изображение на экране монитора	СИ9
6	Побочные сигналы, которые возникают в процессе функционирования технических средств.	Электромагнитное излучение, Токи в сетях связи и электропитания	СИ10
7	Резервные копии файлов с защищаемой информацией, которые могут создаваться в процессе обработки этих файлов	Файлы на жестких дисках ТС	СИ11
8	Остаточная информация на носителях информации	Остаточная информация на жестких дисках ТС	СИ12
		Остаточная информация на съемных носителях информации	СИ13

Таблица 4.4– Программное обеспечение

№ п/п	Программное обеспечение	Обозначение
1	Операционная система ТС, включая все ее компоненты, необходимые для работы	ПО1
2	Средство ИС, включая все его компоненты, установленные на разных ТС ИС	ПО2
3	СКЗИ, выполняющее функции СКЗИ и средства ЭП	ПО3
4	СУБД	ПО4

5	Антивирусное СЗИ	ПО5
6	Пакет программ управления МЭ	ПО6
7	Программа управления шаблонами контроля целостности	ПО7
8	СЗИ от НСД	ПО8
9	Операционная система и иные программные компоненты МЭ	ПО9

Таблица 4.5– Технические средства

№ п/п	Технические средства	Обозначение
1	Файловый сервер	ТС1
2	Web-серве	ТС2
3	АРМ	ТС3
4	Межсетевой экран	ТС4
5	Терминал управления почтовым и web-серверами	ТС5
6	Источник бесперебойного питания	ТС6
7	Коммутатор	ТС7
8	Сетевые кабели между компонентами ИССИБ	ТС8
9	Сетевые кабели, соединяющие компоненты ИССИБ с КИС	ТС9
10	Принтер	ТС10
11	Съемные носители информации для резервного копирования	ТС11
12	Съемные носители информации для хранения ключевой информации	ТС12
13	Съемные носители информации для передачи данных	ТС13
14	Линии электропитания и заземления	ТС14
15	Линии охранной и пожарной сигнализации	ТС15

Защищаемую информацию можно сгруппировать по объектам доступа на программном и аппаратном уровнях (таблица 4.6) [14].

Таблица 4.6 – Объекты доступа

Защищаемая информация	Объект доступа на программном уровне	Объект доступа на аппаратном уровне
ЗИ1, ЗИ3, СИ3	Области оперативной памяти	Модули оперативной памяти ТС
ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, СИ11	Базы данных и отдельные файлы	Жесткие диски ТС
СИ12		Жесткие диски ТС
ЗИ2, ЗИ4, СИ2	Файлы	Съемные защищенные носители информации
ЗИ6, ЗИ10, ЗИ15	Базы данных	Съемные носители информации для целей резервирования информации
ЗИ17, ЗИ20, СИ13	Файлы	Съемные носители информации для целей переноса информации
ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8	Сетевые пакеты	Сетевые кабели
ЗИ8, ЗИ13, СИ5, СИ9	-	Монитор
СИ10	-	ТС, сетевые кабели
ЗИ12	-	МФУ

Основными характеристиками безопасности являются конфиденциальность, целостность и доступность[17]. Характеристики безопасности защищаемой информации ИС представлены в таблице 4.7, программного обеспечения – в таблице 4.8, технических средств – в таблице 4.9.

Таблица 4.7 – Характеристика безопасности ЗИ

№ п.п	Объект угроз	Характеристика безопасности		
		Конфиденциальность	Целостность	Доступность
1	ЗИ1	+	+	-
2	ЗИ2	+	+	-
3	ЗИ3	+	+	-
4	ЗИ4	+	+	+
5	ЗИ5	+	+	+
6	ЗИ6	+	+	+
7	ЗИ7	+	+	+
8	ЗИ8	+	-	+
9	ЗИ9	-	+	+

10	ЗИ10	-	+	+
11	ЗИ11	-	+	+
12	ЗИ12	-	-	+
13	ЗИ13	-	-	+
14	ЗИ14	-	+	+
15	ЗИ15	-	+	+
16	ЗИ16	-	+	+
17	ЗИ17	-	+	+
18	ЗИ18	-	+	+
19	ЗИ19	-	+	+
20	ЗИ20	-	+	+
21	СИ1	+	+	+
22	СИ2	+	+	+
23	СИ3	+	-	-
24	СИ4	-	+	+
25	СИ5	-	-	+
26	СИ6	-	+	+
27	СИ7	-	+	+
28	СИ8	-	+	+
29	СИ9	-	-	+
30	СИ10	+	-	-
31	СИ11	+	-	-
32	СИ12	+	-	-
33	СИ13	+	-	-

Таблица 4.8 – Характеристика безопасности ПО

№ п.п	Объект	Характеристика безопасности

	угроз	Конфиденциальность	Целостность	Доступность
1	ПО1	-	+	+
2	ПО2	-	+	+
4	ПО3	-	+	+
3	ПО4	-	+	+
5	ПО5	-	+	+
6	ПО6	-	+	+
7	ПО7	-	+	+
8	ПО8	-	+	+
9	ПО9	-	+	+

Таблица 4.9 – Характеристика безопасности ТС

№ п.п	Объект угроз	Характеристика безопасности		
		Конфиденциальность	Целостность	Доступность
1	ТС1	-	+	+
2	ТС2	-	+	+
4	ТС3	-	+	+
3	ТС4	-	+	+
5	ТС5	-	+	+
6	ТС6	-	+	+
7	ТС7	-	+	+
8	ТС8	-	+	+
9	ТС9	-	+	+
10	ТС10	-	+	+
11	ТС11	-	+	+
12	ТС12	-	+	+
13	ТС13	-	+	+
14	ТС14	-	+	+
15	ТС15	-	+	+
16	ТС16	-	+	+

Нарушение характеристик безопасности ТС может привести к нарушениям характеристик безопасности ПО, ЗИ и СИ, обрабатываемой на данном ТС или с его помощью.

Нарушение характеристик безопасности ПО может привести к нарушению доступности ЗИ и СИ, обрабатываемой при помощи данного ПО.

Соотношение ТС, ПО, ЗИ и СИ представлено в таблице 4.10.

Таблица 4.10 - Соотношение ТС, ПО, ЗИ и СИ

Техническое средство	Функционирующее ПО	Обрабатываемая, хранящаяся, передаваемая информация	
		Защищаемая информация	Сопутствующая информация
ТС1	ПО1, ПО2, ПО3, ПО5, ПО7, ПО8	ЗИ9, ЗИ14, ЗИ18	СИ1, СИ4, СИ7, СИ10
ТС2	ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8	ЗИ5, ЗИ9, ЗИ14, ЗИ18	СИ1, СИ4, СИ7, СИ10, СИ11, СИ12
ТС3	ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8	ЗИ1, ЗИ3, ЗИ8, ЗИ9, ЗИ13, ЗИ14	СИ3, СИ4, СИ7, СИ10
ТС4	-	-	СИ4, СИ7
ТС5	ПО9	-	СИ4, СИ7, СИ10
ТС6	-	-	СИ5, СИ9, СИ10
ТС8	-	ЗИ7, ЗИ11, ЗИ16, ЗИ19	СИ6, СИ8, СИ10
ТС9	-	ЗИ7, ЗИ11, ЗИ16, ЗИ19	СИ6, СИ8, СИ10
ТС10	-	ЗИ11, ЗИ16, ЗИ19	-
ТС11	-	ЗИ12	-
ТС12	-	ЗИ6, ЗИ10, ЗИ15	-
ТС13	-	ЗИ2, ЗИ4	СИ2, СИ13
ТС14	-	ЗИ17, ЗИ20	-

Данные таблицы созданы и упорядочены опираясь на базовую модель угроз ФСТЕК. Угроза безопасности объекта – возможное нарушение характеристики безопасности объекта.

Разработаем модель угроз безопасности ИС. Все рассмотренные в данном разделе угрозы могут повлечь в той или иной мере случайное нарушение характеристик безопасности ИС. Заинтересованные нарушитель и умысел на нарушение характеристик безопасности в данном случае отсутствует. Поэтому если воздействие данной угрозы непосредственно не приводит к нарушению характеристики безопасности, то считается, что данной угрозы нет. Перечень угроз, не являющихся атаками, приведен в таблице 4.11 [14].

Таблица 4.11 – Список угроз, не являющихся атаками

№ п.п.	Описание угрозы	Обозначение
1	Угрозы, не связанные с деятельностью человека: стихийные бедствия и природные явления (наводнения, ураганы, заморозки и т.д.)	
1.1	Отключение электропитания ТС	У1
1.2	Повреждения ТС от механических воздействий	У2
1.3	Повреждения ТС от скачков напряжения	У3
1.4	Повреждения ТС от пожара, наводнения, обрушения	У4
1.5	Нарушение внешних каналов связи	У5
2	Угрозы социально–политического характера: забастовки, саботаж, локальные конфликты и т.д	
2.1	Отключение электропитания ТС	У1
2.2	Нарушение внешних каналов связи	У5
3	Угрозы техногенного характера	
3.1	Аварии (отключение электропитания, системы заземления, разрушение инженерных сооружений и т.д.)	
3.1.1	Отключение электропитания ТС	У1
3.1.2	Повреждения ТС от механических воздействий	У2
3.1.3	Повреждения ТС от скачков напряжения	У3
3.1.4	Повреждения ТС от пожара	У4
3.2	Неисправности, сбои аппаратных средств, нестабильность параметров системы электропитания, заземления и т.д	
3.2.1	Неисправности ТС	У6
3.2.2	Сбои ТС	У7
3.2.3	Отключение электропитания ТС	У1
3.2.4	Повреждения ТС от скачков напряжения	У3
3.3	Помехи и наводки, приводящие к сбоям в работе аппаратных средств	У7
4	Ошибочные действия и (или) нарушения каких-либо требований технологического процесса обработки информации и защиты информации лицами, санкционировано взаимодействующими с возможными объектами угроз	
4.1	Непредумышленное искажение или удаление программных компонентов ИССИБ, включая файлы конфигурационной информации	У8
4.2	Внедрение и использование неучтенных программ	
4.2.1	Искажение или удаление программных компонентов ИСвредоносной программой	У9
4.2.2	Искажение или удаление ЗИ, обрабатываемой на ТС, вредоносной программой	У10
4.2.3	Искажение или удаление ЗИ со съемных носителей информации вредоносной программой во время их подключения к ТС	У11

4.2.4	Передача ЗИ или СИ вредоносной программой с ТС ИС на внешние сетевые ресурсы	У12
4.2.5	Изменение управляющей информации на ТС вредоносной программой	У13
4.2.6	Нехватка ресурсов ОС в результате действий неучтенной (в т.ч. вредоносной) программы	У14
4.2.7	Отключение ТС в результате действий вредоносной программы	У15
4.3	Игнорирование организационных ограничений (установленных правил) при работе с ресурсами ИС, включая средства защиты информации	
4.3.1	Нарушение правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации)	
4.3.1.1	Повреждения съемных носителей ключевой информации	У16
4.3.1.2	Утеря или передача съемных носителей ключевой информации посторонним лицам	У17
4.3.2	Предоставление посторонним лицам возможности доступа к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований	
4.3.2.1	Механические повреждения СЗИ	У18
4.3.2.2	Изменение настроек СЗИ или системного ПО на ТС, приводящие к невыполнению СЗИ своих функций	У19
4.3.2.3	Отключение СЗИ	У20
4.3.2.4	Непредумышленное искажение или удаление программных компонентов СЗИ	У21
4.3.2.5	Непредумышленное искажение или удаление журналов событий СЗИ	У22
4.3.2.6	Механическое повреждение ТС	У2
4.3.2.7	Внедрение и использование неучтенных программ	У9-У15
4.3.3	Настройка и конфигурирование средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, в нарушение нормативных и технических документов	
4.3.3.1	Изменение настроек СЗИ или системного ПО на ТС, приводящие к невыполнению СЗИ своих функций	У19

Защита от этого типа угроз осуществляется путем проведения соответствующих организационных (в том числе: разработка и применение регламентов работы, инструкций, соблюдение требований технической и эксплуатационной документации, периодический контроль состояния защищенности ИС и проч.) и инженерно-технических (в том числе: использование источников резервного и бесперебойного питания, надежных технических средств и проч.) мероприятий. Меры предотвращения угроз приведены в таблице 4.12 [14].

Таблица 4.12 – Меры предотвращения угроз

№ п.п.	Мера предотвращения угрозы	Обозначение

1	2	3
1	Использование ИБП (ТС7)	МПУ1
2	Размещение ТС в специально оборудованном помещении, ограничение и контроль доступа в помещение. Оснащение помещений ИС охранной сигнализацией	МПУ2
3	Использование зеркального дискового массива	МПУ3
4	Резервирование ЗИ и программной среды ее обработки на внешние носители информации	МПУ4
5	Хранение съемных носителей защищаемой информации в запираемых металлических шкафах/сейфах	МПУ5
6	Оснащение помещений ИС системой противопожарной сигнализации	МПУ6
7	Ограничения полномочий доступа пользователей к системным файлам ОС, файлам настроек СЗИ, СКЗИ	МПУ7
8	Использование антивирусного СЗИ (ПО5) для блокирования действий вредоносных программ. Утверждение перечня разрешенного ПО	МПУ8 (ПО5)
9	Использование СЗИ от НСД и СКЗИ (ТС4, ПО8, ПО3) для контроля целостности файлов	МПУ9 (ТС4, ПО8, ПО3)
10	Использование встроенных в ПО механизмов контроля целостности своих компонентов и конфигурационной информации	МПУ10
11	Установка обновлений безопасности ОС для устранения возможных уязвимостей ОС	МПУ11
12	Обеспечение защищенного хранения и уничтожения ключей в оперативной памяти с помощью СКЗИ (ПО3)	МПУ12 (ПО3)
13	Настройка МЭ (ТС5) для ограничения потоков передачи данных между компонентами ИССИБ и внешней сетью	МПУ13
14	Использование пин-кодов/паролей для доступа к данным на съемном ключевом носителе	МПУ14
15	Организационно-распорядительные документы, регламентирующие технологические процессы обработки информации, порядок обращения с ТС и СЗИ, носителями информации, правила работы в ИС	МПУ15
16	Использование электронной подписи для контроля целостности файлов	МПУ16
17	Установка ТС в запираемые металлические серверные шкафы	МПУ17
18	Периодический контроль соответствия ИССИБ параметрам безопасности	МПУ18
19	Взаимодействие с провайдерами, предоставляющие каналы связи для доступа в сеть общего пользования	МПУ19

Детализированная модель угроз безопасности, не являющихся атаками, и мер по их предотвращению представлена в таблице 4.13.

Таблица 4.13 - Детализированная модель угроз безопасности

Угроза	Объекты угрозы	Нарушаемая характеристика безопасности объекта	Меры предотвращения нарушения характеристик безопасности

			объекта
У1	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6 (СИ5, СИ9), ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС10 (ЗИ11, ЗИ16, ЗИ19), ТС11 (ЗИ12)	Доступность	МПУ1
У2	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ1, ЗИ3, ЗИ9, ЗИ14, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6, ТС7, ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС10 (ЗИ7, ЗИ11, ЗИ16, ЗИ19), ТС11	Целостность	МПУ2, МПУ15, МПУ17
У2	ТС12 (ЗИ6, ЗИ10, ЗИ15), ТС13 (ЗИ2, ЗИ4, СИ2), ТС14 (ЗИ17, ЗИ20)	Целостность	МПУ5 МПУ15 МПУ17
У2	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6 (СИ5, СИ9), ТС7, ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС10 (ЗИ11, ЗИ16, ЗИ19), ТС11 (ЗИ12)	Доступность	МПУ2 МПУ3 МПУ4
У2	ТС12 (ЗИ6, ЗИ10, ЗИ15), ТС13 (ЗИ4, СИ2), ТС14 (ЗИ17, ЗИ20)	Доступность	МПУ5
У3	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ1, ЗИ3, ЗИ9, ЗИ14, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6, ТС11	Целостность	МПУ1 МПУ3 МПУ4
У3	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7),	Доступность	МПУ1 МПУ3 МПУ4

	ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6 (СИ5, СИ9), ТС7, ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС10 (ЗИ7, ЗИ11, ЗИ16, ЗИ19), ТС11 (ЗИ12)		
У4	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ1, ЗИ3, ЗИ9, ЗИ14, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6, ТС7, ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8,), ТС10 (ЗИ7, ЗИ11, ЗИ16, ЗИ19), ТС11	Целостность	МПУ4 МПУ5 МПУ6 МПУ17
У4	ТС12 (ЗИ6, ЗИ10, ЗИ15), ТС13 (ЗИ2, ЗИ4, СИ2), ТС14 (ЗИ17,ЗИ20)	Целостность	МПУ6 МПУ17
У4	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6 (СИ5, СИ9), ТС7, ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС10 (ЗИ11, ЗИ16, ЗИ19) ТС11 (ЗИ12)	Доступность	МПУ4 МПУ6 МПУ17
У4	ТС12 (ЗИ6, ЗИ10, ЗИ15), ТС13 (ЗИ4, СИ2), ТС14 (ЗИ17, ЗИ20)	Доступность	МПУ6
У5	ЗИ7, ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ19
У6	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ1, ЗИ3, ЗИ9, ЗИ14, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6, ТС7, ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС10 (ЗИ11, ЗИ16, ЗИ19) ТС11 (ЗИ12), ТС11	Целостность	МПУ3 МПУ4
У6	ТС12 (ЗИ6, ЗИ10, ЗИ15), ТС13 (ЗИ2, ЗИ4, СИ2), ТС14 (ЗИ17, ЗИ20)	Целостность	МПУ6 МПУ17
У6	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7),	Доступность	МПУ3 МПУ4

	ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6 (СИ5, СИ9), ТС7, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19, ТС11 (ЗИ12)		
У6	ТС12 (ЗИ6, ЗИ10, ЗИ15), ТС13 (ЗИ4, СИ2), ТС14 (ЗИ17, ЗИ20)	Доступность	МПУ6
У7	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7), ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), ТС8 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС6 (СИ5, СИ9), ТС7, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19, ТС11 (ЗИ12)	Доступность	МПУ3 МПУ4
У8	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, СИ4, СИ7	Целостность	МПУ7 МПУ8 (ПО5) МПУ9 (ТС4, ПО8, ПО3) МПУ10 МПУ15 МПУ18
У8	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7, ТС4, СИ6 от ТС5, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ7 МПУ8 (ПО5) МПУ9 (ТС4, ПО8, ПО3) МПУ10 МПУ15 МПУ18 МПУ4
У9	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, СИ4, СИ7	Целостность	МПУ7 МПУ8 (ПО5) МПУ9 (ТС4, ПО8, ПО3) МПУ10 МПУ11
У9	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7, ТС4, СИ6 от ТС5, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ7 МПУ8 (ПО5) МПУ9 (ТС4, ПО8, ПО3) МПУ10 МПУ11
У10	На ТС1: ЗИ9, ЗИ14, ЗИ18, На ТС2: ЗИ5, ЗИ9, ЗИ14, ЗИ18, На ТС3: ЗИ1, ЗИ3, ЗИ9, ЗИ14, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, На ТС10: ЗИ11, ЗИ16, ЗИ19	Целостность	МПУ8 (ПО5) МПУ4 МПУ11 МПУ12 (ПО3) МПУ16
У10	На ТС1: ЗИ9, ЗИ14, ЗИ18, На ТС2: ЗИ5, ЗИ9, ЗИ14, ЗИ18, На ТС3: ЗИ8, ЗИ9, ЗИ14, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ8 (ПО5) МПУ11
У11	На ТС12: ЗИ6, ЗИ10, ЗИ15,	Целостность	МПУ8 (ПО5)

	На ТС13: ЗИ2, ЗИ4, На ТС14: ЗИ17, ЗИ20		МПУ11 МПУ16
У11	На ТС12: ЗИ6, ЗИ10, ЗИ15, На ТС13: ЗИ2, ЗИ4, На ТС14: ЗИ17, ЗИ20	Доступность	МПУ8 (ПО5) МПУ11
У12	На ТС1: СИ1, На ТС2: ЗИ5, СИ1, СИ11, СИ12, На ТС3: ЗИ1, ЗИ3, ЗИ8, СИ3	Конфиденциальность	МПУ8 (ПО5) МПУ11 МПУ12 (ПО3) МПУ13 (ТС5)
У13	СИ4 на ТС1, ТС2, ТС3, СИ6 на ТС9	Целостность	МПУ8 (ПО5) МПУ11
У13	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7, ТС4, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ8 (ПО5) МПУ11
У14	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7, ТС4, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ8 (ПО5) МПУ11
У15	ТС1 (ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС2 (ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7), ТС3 (ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7), ТС6 (СИ5, СИ9) ТС9 (ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8), ТС10 (ЗИ11, ЗИ16, ЗИ19), ТС11 (ЗИ12)	Доступность	МПУ8 (ПО5) МПУ11
У16	ТС13 (СИ2)	Целостность	МПУ4
У16	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7, На ТС4: СИ4, СИ7, На ТС5: ПО9, СИ4, СИ7, ТС6 (СИ5, СИ9) На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ4
У17	СИ2 на ТС13	Конфиденциальность	МПУ4 МПУ14
У17	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8,ЗИ9, ЗИ14, СИ4, СИ7, На ТС4: СИ4, СИ7, На ТС5: ПО9, СИ4, СИ7,	Доступность	МПУ4

	ТС6 (СИ5, СИ9), На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19		
У18	ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7)	Целостность	МПУ15
У18	ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8 На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ15
У19	СИ4 на ТС1, ТС2, ТС3, ТС4, ТС5 СИ6 на ТС9, ТС10	Целостность	МПУ15
У19	ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ15 МПУ4
У20	ТС4 (СИ4, СИ7), ТС5 (ПО9, СИ4, СИ7), На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ4, СИ7, На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ15
У21	На ТС1: ПО3, ПО5, ПО7, ПО8, На ТС2: ПО3, ПО5, ПО7, ПО8, На ТС3:ПО3, ПО5, ПО6, ПО7, ПО8, На ТС5: ПО9,	Целостность	МПУ15 МПУ7 МПУ9 (ТС4, ПО8, ПО3) МПУ10
У21	На ТС1: ПО1, ПО2, ПО3, ПО5, ПО7, ПО8, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС2: ПО1, ПО2, ПО3, ПО4, ПО5, ПО7, ПО8, ЗИ5, ЗИ9, ЗИ14, ЗИ18, СИ1, СИ4, СИ7, На ТС3: ПО1, ПО2, ПО3, ПО5, ПО6, ПО7, ПО8, ЗИ8, ЗИ9, ЗИ14, СИ3, СИ4, СИ7, ТС4, ТС5 (ПО9, СИ4, СИ7), На ТС9: ЗИ7, ЗИ11, ЗИ16, ЗИ19, СИ6, СИ8, На ТС10: ЗИ11, ЗИ16, ЗИ19	Доступность	МПУ15 МПУ7 МПУ9 (ТС4, ПО8, ПО3) МПУ10
У22	СИ7 на ТС1, ТС2, ТС3, ТС4, ТС5, СИ8 на ТС9	Целостность	МПУ15
У22	СИ7 на ТС1, ТС2, ТС3, ТС4, ТС5, СИ8 на ТС9	Доступность	МПУ15

В результате составления модели угроз можно сделать вывод, что реализация угроз У16 — У22 может приводить к невыполнению функций СЗИ, для которых они предназначены, а, следовательно, снижать уровень защищенности ИС, повышать уровень актуальности других угроз (в качестве мер противодействия которым использовались СЗИ) и создавать условия для проведения атак на объекты угроз заинтересованным нарушителем.

Для рассмотрения всех возможных последствий реализации угроз У16 — У22 (нарушений характеристик безопасности объектов угроз) следует также рассматривать возможные последствия реализации всех угроз, среди мер противодействия которым указаны СЗИ (У8 — У15).

Угроза нарушения конфиденциальности остаточной информации (СИ12 — СИ13) актуальна только в случае передачи электронных носителей, на которых ранее была зафиксирована защищаемая конфиденциальная информация, третьим лицам при условии наличия заинтересованности этих лиц в получении такой информации.

При разработке модели нарушителя учитывались следующие положения:

− безопасность защищаемой информации в ИС обеспечивается средствами защиты информации, а также используемыми в ИС информационными технологиями, техническими и программными средствами, удовлетворяющими требованиям по защите информации, устанавливаемым в соответствии с законодательством Российской Федерации;

− средства защиты информации (СЗИ) штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к ним требований;

− СЗИ не могут обеспечить защиту ЗИ от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СЗИ не может обеспечить защиту данных от раскрытия лицами, которым предоставлено право на доступ к этим данным).

− принимается, что нарушитель не может действовать на этапах разработки, производства, хранения и транспортировки ТС, ПО, СЗИ и СКЗИ, которые сертифицированы в системе сертификации ФСБ России или ФСТЭК России (т.е. имеют положительное заключение экспертной организации о соответствии требованиям нормативных документов по безопасности информации).

Атаки являются наиболее опасными угрозами, что обусловлено их тщательной подготовкой, скрытностью проведения, целенаправленным выбором объектов и целей атак. Атаки готовятся и проводятся нарушителем, причем конкретные возможности нарушителя определяют конкретные атаки, которые может провести нарушитель. В качестве атаки рассматриваются только преднамеренные посягательства нарушителя на ИССИБ, ее компоненты и (или) защищаемую информацию, с целью нарушения характеристик безопасности информации.

Рассматриваются следующие виды атак: [13]

- прямые угрозы, т.е. атаки, осуществление которых непосредственно нарушает характеристики безопасности ЗИ;

- косвенные угрозы, т.е. атаки, создающие условия для появления прямых угроз.

Объекты атак:

- ЗИ обрабатывается и хранится в ИС с использованием технических средств и информационных технологий, которые порождают объекты защиты различного уровня. Атаки на эти объекты создают прямые и косвенные угрозы.

Таким образом, объектом атаки может выступать: защищаемая информация; сопутствующая информация; программное обеспечение ИС; технические средства ИС.

В качестве нарушителей (субъектов атак) безопасности ИС рассматриваются физические лица. Все потенциальные нарушители подразделяются на:

- внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны ИС;

- внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны ИС.

С точки зрения наличия права постоянного или разового доступа в контролируемую зону (КЗ) объектов размещения ИС- все физические лица могут быть отнесены к следующим двум категориям: категория I - лица, не имеющие права доступа в контролируемую зону; категория II - лица, имеющие право доступа в контролируемую зону. К внутренним нарушителям относятся только лица II категории. К внешним нарушителям относятся лица I категории и лица категории II, находящиеся за пределами КЗ. Распределение групп нарушителей приведены в таблице 4.14.

Таблица 4.14 – Распределение групп нарушителей

№ п.п.	Группа	Категория	Внутренний	Внешний	Условное обозначение
1	Работники				
1.1	Администратор безопасности	II	+	+	СА1
1.2	Операторы	II	+	+	СА2
2	Системный администратор	II	+	+	СА3
3	Работники компании, осуществляющие техническое обслуживание помещений	II	+	+	СА4
4	Работники сторонних организаций, обслуживающие ТС	II	+	+	СА5
5	Работники компании, не имеющие права доступа в КЗ	II	+	+	СА6
6	Клиенты-пользователи файлового сервера	II	+	+	СА7
7	Работники и поставщики сертифицированных	I	-	+	СА8

	ТС, ПО, СКЗИ, СЗИ				
8	Работники сторонних организаций, осуществляющие поставку и ремонт прочих ТС и ПО ИС	I	-	+	CA9
9	Внешние нарушители, не относящиеся к другим категориям	I	-	+	CA10

Привилегированные пользователи информационной системы, назначенные из числа особо доверенных лиц и осуществляющие техническое обслуживание технических и программных средств ИС, СЗИ, СКЗИ, включая их настройку, конфигурирование и распределение ЗИ и СИ между привилегированными пользователями, а также лица I категории, исключаются из числа потенциальных нарушителей по следующим основаниям (таблица 4.15).

Таблица 4.15 – Основания на исключение из числа потенциальных нарушителей

№ п.п	Субъект атаки	Обоснование
1	CA1	Администратор безопасности исключается из числа потенциальных нарушителей, так как заинтересован в соблюдении характеристик безопасности ИС.
2	CA2	Оператор АС не является потенциальным нарушителем, так как является доверенным лицом, заинтересованным в соблюдении характеристик безопасности ИС.
3	CA3	Системный администратор не является потенциальным нарушителем, так как является доверенным лицом, заинтересованным в соблюдении характеристик безопасности ИС.
4	CA8	Разработчики сертифицированных ТС, ПО, СКЗИ, СЗИ исключаются из числа потенциальных нарушителей, как доверенные лица, прошедшие проверку в рамках системы сертификации ФСБ РФ

Возможность сговора потенциальных нарушителей представлена в таблице 4.16.

Таблица 4.16 - Возможность сговора потенциальных нарушителей

Субъект	CA4	CA5	CA6	CA7	CA9	CA10
CA4	-	-	+	-	-	+
CA5	-	-	+	-	-	+

CA6	+	+	-	+	+	+
CA7	-	-	+	-	-	-
CA9	-	-	+	-	-	-
CA10	+	+	+	-	-	-

Примечание:

«-» - сговор между субъектами атаки не возможен по разным причинам: субъекты не могут иметь общих интересов; субъекты не встречаются в реальности; сферы деятельности субъектов не позволяют им действовать сообща; крайне низкая вероятность сговора; либо сговор между субъектами атаки возможен но: не позволяет объединить знания и (или) возможности для проведения совместной атаки; не дает новых знаний и (или) возможностей для проведения атаки;

«+» - сговор между субъектами атаки возможен и позволяет реализовать одну или несколько атак.

Таким образом, учитывая возможности сговора, получаем актуальный перечень субъектов атак на ИС (таблица 4.17).

Таблица 4.17 – Актуальный перечень субъектов атак

№ п.п.	Описание	Условное обозначение
1	Работники, осуществляющие техническое обслуживание помещений	CA4
2	Работники сторонних организаций, обслуживающие ТС, расположенные в КЗ	CA5
3	Работники, не имеющие права доступа в КЗ	CA6
4	Клиенты - пользователи	CA7
5	Работники сторонних организаций, осуществляющих поставку и ремонт прочих ТС и ПО ИС	CA9
6	Внешние нарушители, не относящиеся к другим категориям	CA10
7	Сговор {«Работники, осуществляющие техническое обслуживание помещений УЦ» и «Работники, не имеющие права доступа в КЗ»}	CA46
8	Сговор {«Работники, осуществляющие техническое обслуживание помещений» и «Внешние нарушители, не относящиеся к другим категориям»}	CA410
9	Сговор {«Работники сторонних организаций, обслуживающие ТС, расположенные в КЗ» и «Работники, не имеющие права доступа в КЗ»}	CA56
10	Сговор {«Работники сторонних организаций, обслуживающие ТС, расположенные в КЗ» и «Внешние нарушители, не относящиеся к другим категориям»}	CA510
11	Сговор {«Работники, не имеющие права доступа в КЗ» и «Клиенты - пользователи УЦ»}	CA67
12	Сговор {«Работники, не имеющие права доступа в КЗ» и «Работники сторонних организаций, осуществляющих поставку и ремонт прочих ТС и ПО ИС»}	CA69
13	Сговор {«Работники, не имеющие права доступа в КЗ» и «Внешние нарушители, не относящиеся к другим категориям»}	CA610

Вероятность появления множественных сговоров намного ниже, чем вероятность появления двусторонних сговоров, поэтому многосторонние сговоры исключаются из рассмотрения [19].

Нарушитель обладает полной информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты и организационными мерами, принятыми на объекте.

Нарушители имеют все необходимые для проведения атак по доступным им каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну. Средства атаки, имеющиеся у нарушителя, представлены в таблице 4.18.

Таблица 4.18 - Средства атаки, имеющиеся у нарушителя

№ п.п.	Средство атаки	Условное обозначение
1	Технические средства ИС, с которыми осуществляется штатное функционирование СКЗИ.	СПА1
2	Доступные в свободной продаже технические средства и программное обеспечение	СПА2
3	Специально разработанные технические средства и программное обеспечение	СПА3
4	Штатные средства ИС	СПА4
5	Специальные технические средства перехвата информации по техническим каналам утечки информации	СПА5

В таблице 4.19 представлены ограничения на имеющиеся у нарушителя средства атаки.

Таблица 4.19 - Ограничения на имеющиеся у нарушителя средства атаки

Средство атаки Субъект атаки	СПА1	СПА2	СПА3	СПА4	СПА5
СА4	-	-	-	-	-
СА5	-	+	+	-	+
СА6	-	+	-	-	-
СА7	-	+	-	-	-
СА9	-	+	+	-	-
СА10	-	+	+	-	+
СА46	-	+	-	-	-
СА410	-	+	+	-	+

СА56	-	+	+	-	+
СА510	-	+	+	-	+
СА67	-	+	-	-	-
СА69	-	+	+	-	-
СА610	-	+	+	-	+

Примечание:
«+» - нарушитель располагает средством атаки;
«-» - нарушитель не располагает средством атаки.

Описание каналов атак представлено в таблице 4.20.

Таблица 4.20 – Описание каналов атак

№ п.п.	Канал атаки	Условное обозначение
1	Каналы связи (как внутри, так и вне контролируемой зоны), не защищенные от НСД к информации организационно-техническими мерами (КИС, подключенная к ИС)	КА1
2	Штатные средства ИС	КА2
3	Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический)	КА3
4	Машинные носители информации	КА4
5	Носители информации, выведенные из употребления	КА5
6	Технические каналы утечки	КА6
7	Сигнальные цепи	КА7
8	Цепи электропитания	КА8
9	Цепи заземления	КА9
10	Канал утечки за счет электронных устройств негласного получения информации	КА10
11	Информационные и управляющие интерфейсы СВТ	КА11

Ограничения на доступ к каналам атаки приведены в таблице 4.21.

Таблица 4.21 – Ограничения на доступ к каналам атаки

Субъект Канал	КА1	КА2	КА3	КА4	КА5	КА6	КА7	КА8	КА9	КА10	КА11

CA4	-	-	-	-	+	-	-	-	-	-	-
CA5	-	-	-	-	+	-	-	+	+	-	-
CA6	+	-	-	-	+	-	-	-	-	-	-
CA7	-	-	-	-	+	-	-	-	-	-	-
CA9	-	-	-	-	+	-	-	-	-	-	-
CA10	-	-	-	-	+	-	-	+	+	-	-
CA46	+	-	-	-	+	-	-	-	-	-	-
CA410	-	-	-	-	+	-	-	+	+	-	-
CA56	+	-	-	-	+	-	-	+	+	-	-
CA510	-	-	-	-	+	-	-	+	+	-	-
CA67	+	-	-	-	+	-	-	-	-	-	-
CA69	+	-	-	-	+	-	-	-	-	-	-
CA610	+	-	-	-	+	-	-	+	+	-	-

Примечание:

«+» - нарушитель имеет возможность воспользоваться каналом атаки;

«-» - нарушитель не имеет возможности воспользоваться каналом атаки.

Каналы связи, не защищенные от НСД к информации организационно-техническими мерами, – такой канал связи присутствует только между ИС и корпоративной информационной сетью. По данному каналу не передается конфиденциальная информация. Доступ к компонентам ИС по данному каналу ограничивается межсетевым экраном. Каналы связи между компонентами ИС расположены в пределах границ КЗ, а передаваемая в них информация защищена СКЗИ.

Каналы непосредственного доступа к объекту атаки (акустический, визуальный, физический) – возможность реализации атаки потенциальным нарушителем ограничена применением комплекса режимных мероприятий, в том числе: ограничение доступа в помещения ИС, контроль работников УЦ за лицами, присутствующими в помещениях, применение технических средств защиты, контроль вскрытия. По акустическому каналу связи конфиденциальная информация не передается [18].

Материальные носители информации – канал актуален в случае хищения материальных носителей у авторизованного пользователя с целью получения ключевой информации. Возможность реализации атаки ограничена применением комплекса режимных мероприятий, в том числе: ограничение доступа в помещения ИС, хранение электронных носителей

информации в запираемых хранилищах, установление правил обращения с носителями информации.

Носители информации, выведенные из употребления – возможность реализации атаки должна ограничиваться путем гарантированного уничтожения информации, содержащейся на носителях, либо уничтожением самих носителей.

Сигнальные цепи, цепи электропитания, цепи заземления – объем информации, который может быть получен в результате успешной реализации атаки крайне ограничен, что несопоставимо со сложностью реализации и затратами на проведение атаки.

Канал утечки за счет электронных устройств негласного получения информации. Доступ в контролируемую зону ограничен в соответствии с внутренними документами Общества. По акустическому каналу связи конфиденциальная информация не передается.

Информационные и управляющие интерфейсы СВТ – недоступны потенциальному нарушителю, защищены средствами, описанными в предыдущих разделах, а также организационными мерами [17].

Каналы утечки подлежащей защите информации, содержащейся в побочных сигналах, возникающих при функционировании криптосредств – объем информации, который может быть получен в результате успешной реализации атаки крайне ограничен, что несопоставимо со сложностью реализации и затратами на проведение атаки.

Исходя из выявленных возможностей, устанавливаются следующие типы нарушителей, представленные в таблице 4.22

Таблица 4.22 – Типы нарушителей

Субъект атаки	Категория	Внутренний	Внешний	Тип нарушителя
СА4	II	+	+	Н2
СА5	II	+	+	Н2
СА6	II	+	+	Н2
СА7	II	+	+	Н2
СА9	I	-	+	Н1
СА10	I	-	+	Н1
СА46	II	+	+	Н2
СА410	II	+	+	Н2
СА56	II	+	+	Н2
СА510	II	+	+	Н2
СА67	II	+	+	Н2

CA69	II	+	+	H2
CA610	II	+	+	H2

Для создания модели нарушителя информационной безопасности была использована базовая модель нарушителя ФСТЭК. Таким образом, для объекта информатизации АО «Дальневосточная генерирующая компания» в г. Хабаровске актуален нарушитель, относящийся к типу H2 – внутренний нарушитель, имеющий право доступа в контролируемую зону, но не имеющий свободного доступа к компонентам ИС. Для закрытия выявленных каналов атак используются сертифицированные СЗИ от НСД, МЭ, СКЗИ, а также применяются соответствующие организационные меры, описанные в настоящей Модели угроз.

Необходимость в средствах обнаружения атак отсутствует ввиду того, что ИСС не имеет штатных средств, расположенных за пределами КЗ, и доступ из внешних по отношению к ИС сетей ограничен межсетевым экраном.

Угроза утечки информации конфиденциального характера по техническим каналам признана неактуальной (не опасной) ввиду указанных причин.

5. Общие рекомендации по улучшению защищенности предприятия

Виртуальные частные сети обладают несколькими характеристиками [7]:

- трафик шифруется, обеспечивая тем самым, защиту от несанкционированного доступа;
- имеется аутентификация удаленного клиента;

- обеспечивается поддержка большого количества протоколов;

- соединение обеспечивается на основе связи только с двумя конкретными абонентами.

Реализация VPN осуществляется двумя типовыми способами.

Remote VPN. VPN в режиме удаленного доступа. Данная типовая схема подключения представлена на рисунке 5.1. Режим подключения ориентируется на удаленную работу одиночного пользователя с локальной сетью Компании.

Пользователь, подключается к сети Internet доступными ему способами, использует специализированное клиентское программное обеспечение, осуществляется связь с удаленным VPN сервером. VPN сервер шифрует передаваемый трафик и предоставляет пользователю возможность работать в данной сети [9].

При организации корпоративной сети данным способом необходимо с каждого узла осуществлять выделенное VPN соединение. Для обеспечения требований по защите информации, каждый узел оснащается сертифицированным средством защиты, что существенно увеличит стоимость реализации проекта в целом.

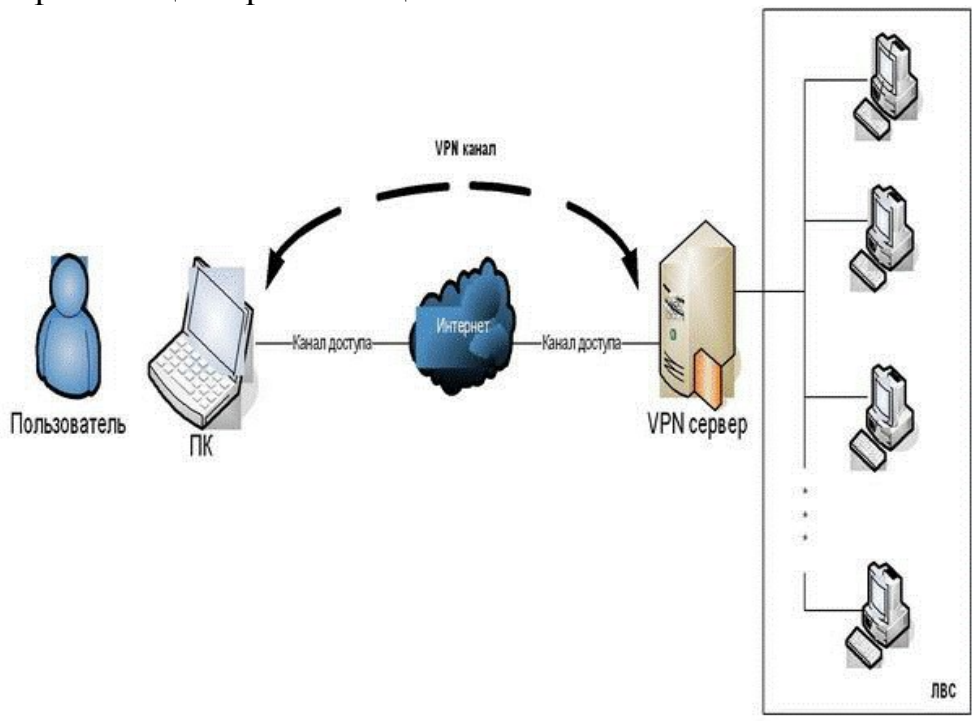

Рисунок 5.1 – VPN в режиме удаленного доступа

Site-to-Site VPN. VPN в данном режиме осуществляет объединение сетей. Типовая схема представлена на рисунке 5.2. Использование VPN данным способом предполагает установку VPN-маршрутизаторов на границе объединения нескольких сетей. При этом работа пользователей осуществляется штатным образом, все задачи по объединению сетей, организации VPN туннелей и маршрутизации выполняется пограничным маршрутизатором.

Для реализации данного режима необходимо обеспечить уникальность сетевых адресов каждого компьютера в пределах корпоративных сетей.

Исходя из выше сказанного, в качестве способа организации VPN корпоративной сети Компании выбирается режим Site-to-Site как наиболее удобный с точки зрения работы пользователей [10].

Для этого необходимо произвести замену существующего оборудования на оборудование с поддержкой VPN.

Из представленных на рынке РК марок оборудования, а так же с учетом фирмы производителя существующего оборудования на сети, было выбрано оборудование компании Cisco.

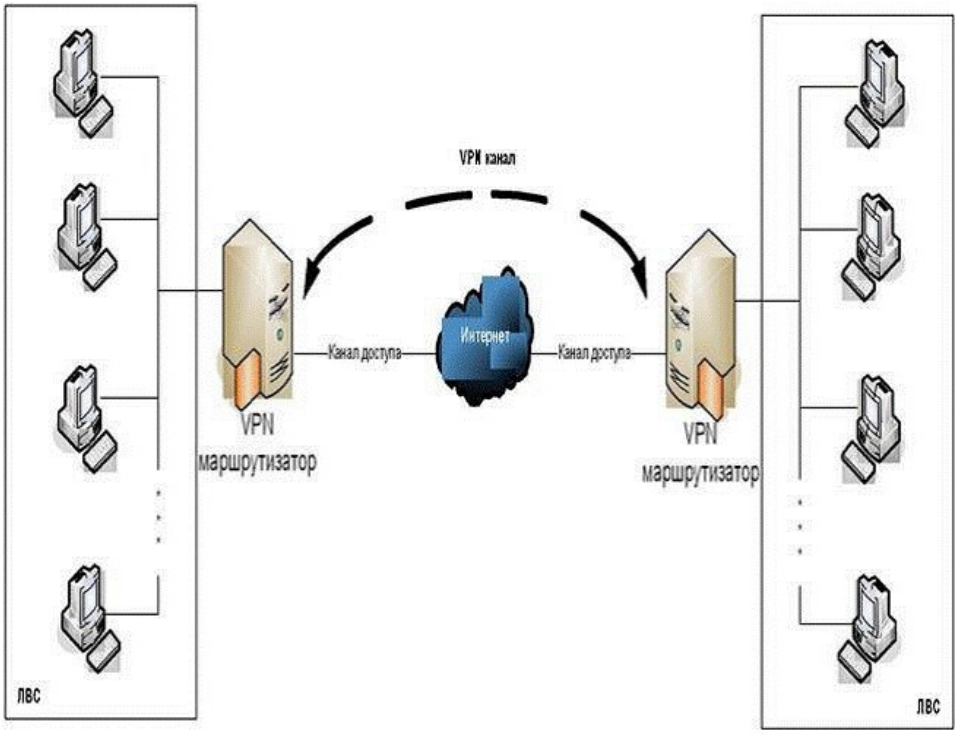

Рисунок 5.2 – VPN в режиме объединения сетей

С учетом выбранной топологии построения сети и оборудования схема проектируемой сети представлена на рисунке 5.3 модель корпоративной виртуальной частной сети VPN АО «Дальневосточная генерирующая компания» в г. Хабаровске на базе решений всемирного фаворита в сфере телекоммуникаций Cisco Systems.

Эта корпоративная сеть способна давать для работников компании все без исключения типы телекоммуникационных услуг и её возможно рассматривать мультисервисной, так как и трафик сведений и голосовой трафик переходят по кодированному каналу VPN. Корпоративная сеть АО «Дальневосточная генерирующая компания» в г. Хабаровске считается излишней и резервируется 2-мя интернет провайдерами, то что допустимо вследствие интегрированной в Cisco IOS функции Cisco IP SLA.

В локальной сети главного офиса АО «Дальневосточная генерирующая компания» в г. Хабаровске нужно 2 коммутатора доступа, для того чтобы

делить поток на 2 канала, нацеленных на главный и запасной маршрутизаторы, чем гарантируется сто процентное резервирование.

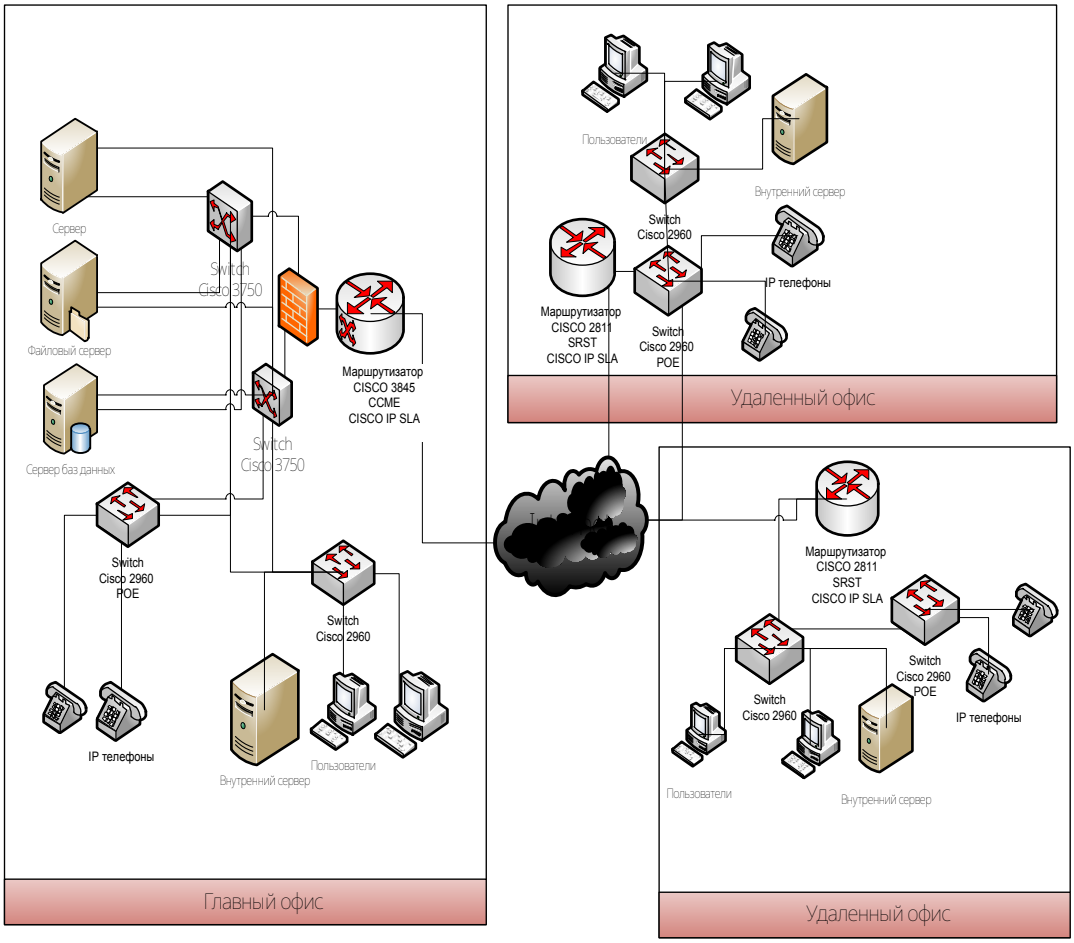

Рисунок 5.3 - Смоделированная корпоративная сеть на базе технологии VPN для АО «Дальневосточная генерирующая компания» в г. Хабаровске

В случае если на 1-ом из маршрутизаторов исчезнет поток от провайдера, в таком случае роутер благодаря функции Cisco IP SLA переключится на 2-ой запасной.

В роли мини-АТС применяется IP–PBX Cisco CallManager Express, встроенный в маршрутизатор Cisco 3845, к который подсоединяются все без исключения IP-телефонные аппараты компании Cisco Systems.

Заключение

В результате анализа корпоративной сети предприятия АО «Дальневосточная генерирующая компания» в г. Хабаровске была дана характеристика объекта, проанализирована существующая информационная система организации. Были определены достоинства и недостатки существующей системы защиты предприятия, разработаны модели угроз и нарушителя.

При разработке плана мероприятий выбраны аппаратная и программная части системы защиты. Выбор был остановлен на продукции компании Cisco Systems. Cisco один из всемирных фаворитов в сфере поставок продуктов, в том числе ПО, а кроме того услуг в области создания и предоставления работы компьютерных сетей. Производственная линия фирмы содержит коммутаторы, маршрутизаторы, приборы удаленного доступа, устройства интернет-сервисов, преобразователи протоколов, ПО управления сетью, которые связываю географически распределенные локальные сети, глобальные сети и непосредственно сеть интернет

Можно сделать вывод, что в результате работы были решены следующие задачи:

- описана и проанализирована компьютерная предприятия;
- выявлены и оценены угрозы, характерные для данной сети;
- проанализирована существующая в АО «Дальневосточная генерирующая компания» в г. Хабаровске система информационной безопасности;
- разработаны меры по улучшению данной системы защиты.

Список литературы

1. Защита данных в компьютерных сетях. [Электронный ресурс]/Инфоурок – Электрон. дан. – Режим доступа: http://vsptus.ru/6.html.
2. Медведовский И.Д. Практическое применение международного стандарта безопасности информационных систем ISO 17799 [Электронный ресурс] / И.Д. Медведовский. – Электрон. Дан. – М.: МЦФ: ИДДК, cop. 2007. – 1 электрон. опт. диск (CD-ROM).
3. Милославская Н.Г. Интрасети: обнаружение вторжений: учеб. пособие для вузов / Н.Г. Милославская, А.И. Толстой – М.: ЮНИТИ-ДАНА, 2001. – 587 с.
4. Гречанинов А.В. DMZ – Каменный мешок для хакера. [Электронный ресурс]/А.В. Гречанинов – Электрон. дан - Режим доступа: http://gretchaninov.com.
5. Тутубалин А. Распределенные методы обнаружения спама [Электронный ресурс]/А. Тутубалин. Электрон. Дан. – Режим доступа: http://www.lexa.ru/lexa/.
6. Медведовский И.Д. Атака на Internet/И.Д. Медведовский, П.В.Семьянов, Д.Г. Леонов. – М.:ДМК, 2009 г. – 366 с.
7. Система Check Point Firewall-1. [Электронный ресурс]/Инфоурок – Электрон. дан. – Режим доступа: http://www.cnews.ru.
8. Lewis M. Creating a Manageable Security. [Электронный ресурс]/Инфоурок – Электрон. дан. – Режим доступа: http://www.sql.ru/articles/Publications.shtml.
9. Франчук В.И., Основы современной социальной инженерии: Учебник / Франчук В.И – СПб.: БХВ-Петербург, 2010. – 399с.
10. Гольдштейн, Б.С. Сети связи: учебник / Б.С. Гольдштейн, Н.А. Соколов, Г.Г. Яновский. – СПб.: БХВ-Петербург, 2010. – 399с.
11. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)., 2008 год [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god.
12. Базовая модель нарушителя ИБ [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: https://fstec.ru/component/attachments/download/812.
13. Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-

obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god.

14. Федеральный закон РФ «Об электронной подписи» от 06.04.2011 г. № 63-ФЗ[Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: http://www.consultant.ru/

15. Федеральный закон РФ «Об информации, информационных технологиях и защите информации» от 27.07.2006 г. № 149-ФЗ, [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61801.

16. «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» (утверждены руководством 8 Центра ФСБ России, 21.02.2008 г. № 149/54-144). [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа

17. Приказ ФСБ РФ от 27.12.2011 N 796 "Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра" (Зарегистрировано в Минюсте РФ 09.02.2012 N 23191) [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_126209

18. Оценка субъектов интеллектуальной собственности. [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: https://patentural.ru/zhurnal/oczenka-intellektualnoj-sobstvennosti/

19. Подготовительный этап и планирование затрат. [Электронный ресурс]/ФСТЭК России – Электрон. дан. – Режим доступа: http://buh.bobrodobro.ru/4226