Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации

Утверждена распоряжением по институту
от «12» марта 2020 г. № 029-р/12.00
Выполнена по заявке организации
(предприятия)_____
_____

Допущена к защите
« 18 » июня 2020 г.
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ПОСТРОЕНИЮ ЗАЩИЩЕННОЙ РАСПРЕДЕЛЕННОЙ СЕТИ ОРГАНИЗАЦИИ НА БАЗЕ СЕТИ ИНТЕРНЕТ С ИСПОЛЬЗОВАНИЕМ АПКШ «КОНТИНЕНТ»

Рецензенты:
Герасимов Владимир Павлович
канд. техн. наук, доц., доцент кафедры информационных систем и технологий
ФГБОУ ВО «Ставропольский государственный аграрный университет

Нормоконтролер:
Бисюков Виктор Михайлович,
доцент, доцент
кафедры организации и технологии защиты информации

(*подпись*)

Выполнил (а):
Аникин Дмитрий Андреевич
студент 4 курса, группы ИНБ-б-о-16-2 направления подготовки 10.03.01 «Информационная безопасность» профиль «Организация и технология защиты информации» очной формы обучения

(*подпись*)

Руководитель:
Бисюков Виктор Михайлович
доцент, доцент
кафедры организации и технологии защиты информации

(*подпись*)

Дата защиты «30» июня 2020 г.

Оценка _____

Ставрополь, 2020 г.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт	информационных технологий и телекоммуникаций
Кафедра	организации и технологии защиты информации
Направление	Информационная безопасность
Профиль	Организация и технология защиты информации

УТВЕРЖДАЮ
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В. И. Петренко
«04» апреля 2020 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ (ДИПЛОМНУЮ РАБОТУ)

Студент Аникин Дмитрий Андреевич группа ИНБ-б-о 16-2

1. Тема Разработка рекомендаций по построению защищенной распределенной сети организации на базе сети Интернет с использованием АПКШ «Континент»

Утверждена распоряжением по институту «12» марта 2020 г. № 029-р/12.00

2. Срок представления работы к защите «27» июня 2020 г.

3. Исходные данные для выполнения работы Работу выполнить в соответствии с требованиями ФЗ №152-ФЗ «О персональных данных» от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации"

4. Содержание бакалаврской работы:

4.1 Анализ комплексной системы защиты информации ООО «ЭНЕРГО»

4.2 Сравнительный анализ существующих методов и средств реализации VPN-технологий при построении защищенных распределенных сетей

4.3 Рекомендации по построению защищенной распределенной сети организации на базе.

4.4 Технико-экономическое обоснование результатов работы

Приложение А, Б, В, Г, Д

Дата выдачи задания «04» апреля 2020 г.

Руководитель работы _____ (*подпись*) В.М. Бисюков (*инициалы, фамилия*)

Консультанты по разделам

_____ (*подпись*) _____ (*инициалы, фамилия*)

_____ (*подпись*) _____ (*инициалы, фамилия*)

_____ (*подпись*) _____ (*инициалы, фамилия*)

Задание к исполнению принял «04» апреля 2020 г. Д.А. Аникин
подпись

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации
Направление Информационная безопасность
Профиль Организация и технология защиты информации

КАЛЕНДАРНЫЙ ПЛАН

Фамилия, имя, отчество Аникин Дмитрий Андреевич
Тема ВКР Разработка рекомендаций по построению защищенной распределенной сети организации на базе сети Интернет с использованием АПКШ «Континент»
Руководитель Бисюков В.М.
Консультанты:

№	Наименование этапов выполнения выпускной квалификационной работы	Срок выполнения работы	Примечание
1.	Анализ литературы по теме работы	08.04.2020	
2.	Анализ структуры, деятельности и организации защиты персональных данных в ООО «ЭНЕРГО».	15.04.2020	
3.	Организация системы защиты персональных данных в ООО «ЭНЕРГО»	07.05.2020	
4.	Оценка эффективности предложенных рекомендаций и технико-экономическое обоснование результатов работы.	02.06.2020	
5.	Представление ВКР руководителю и нормоконтролёру	05.06.2020	
6.	Предварительная защита	09.06.2020	
7.	Представление ВКР заведующему кафедрой	18.06.2020	
8.	Рецензирование	20.06.2020	
9.	Представление ВКР в ГЭК	27.06.2020	

Руководитель В.М. Бисюков
Зав. кафедрой В.И. Петренко
«04» апреля 2020 г.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

АРМ	–	автоматизированное рабочее место
АС	–	автоматизированная система
ЗПДн	–	защита ПДн
ИБ	–	информационная безопасность
КЗ	–	контролируемая зона
ЛВС	–	локально–вычислительная сеть
НМД	–	нормативно–методические документы
НДВ	–	не декларированные возможности
ПДн	–	персональные данные
ПО	–	программное обеспечение
ППО	–	прикладное программное обеспечение
ПЭМИН	–	побочные электромагнитные излучения и наводки
СВТ	–	средства вычислительной техники
СЗИ	–	средство защиты информации
СЗПДн	–	система защиты ПДн
СКЗИ	–	средства криптографической защиты информации
СП	-	структурные подразделения
СПО	–	системное программное обеспечение
ССОП	–	сети связи общего пользования
СУБД	–	система управления базами данных
СФХ	–	структурно–функциональные характеристики
ТЗ	–	техническое задание
ТСр	–	технические средства
ФСБ	–	Федеральная служба безопасности
ФСТЭК	–	Федеральная служба по техническому и экспортному контролю

ВВЕДЕНИЕ

В настоящее время одним из наиболее востребованных товаров, является информация. Поэтому ее сохранность играет огромную роль как для коммерческих организаций, так и для общества.

Проблема безопасности как в глобальных, так и в локальных сетях усугубляется сложностью применения традиционных методов борьбы с преступлениями. Даже если взлом обнаружен, что происходит очень редко, его далеко не всегда можно проследить до реального злоумышленника, поскольку для взлома может использоваться цепочка машин, принадлежащим разным организациям, возможно, находящимся в разных концах земного шара.

В современных коммерческих организациях, в силу распределенной структуры, за счет множества филиалов, возникает задача защиты информации при ее передаче по каналам связи. Участились случаи, когда компании малого бизнеса становятся жертвами мошенников, которые тем или иным способом использовали похищенную информацию, составляющую коммерческую тайну организации, для получения собственной выгоды. Утечке информации могут способствовать недостатки в системе защиты информации, а также уязвимости оборудования (средств передачи).

Актуальность данной работы обуславливается тем, что организация может стать жертвой сетевых атак, связанных с перехватом информации, в которой может содержаться коммерческая тайна. В силу того, что организация выполняет различные виды деятельности, связанные с обработкой персональных данных клиентов, сведений о юридических лицах, выдаче лицензий, то перехват информации конкурентами и злоумышленниками, может привести к значительным убыткам для организации.

Для защиты информации передаваемой по сетям передачи данных, между составными частями Virtual Private Network (VPN) соединения, при объединении локальных сетей филиалов организации в единую сеть через VPN, а так же для установления защищенного подключение удаленных

пользователей к ресурсам локальной вычислительной сети, предлагается использовать аппаратно-программный комплекс шифрования (АПКШ) «Континент».

Объектом исследования в данной работе является распределенная сеть организации, состоящей из главного офиса и филиала.

Предметом исследования – методы использования технологий VPN при построении защищенных распределенных сетей в организации с помощью АПКШ «Континент».

Целью проведения исследовательской работы является повышение уровня защищенности распределенной сети ООО «ЭНЕРГО», за счет уменьшения риска информационной безопасности, связанного с угрозами несанкционированного доступа и перехватом информации через распределенную сеть, при помощи АПКШ «Континент».

Для достижения вышеуказанной цели необходимо решить ряд задач:

– проанализировать комплексную систему защиты информации организации;

– провести сравнительный анализ существующих методов и средств реализации VPN-технологий при построении защищенных распределенных сетей;

– разработать рекомендации по построению защищенной распределенной сети организации на базе сети Интернет с использованием АПКШ «Континент»;

– составить технико-экономическое обоснование.

Данная выпускная квалификационная работа имеет четыре раздела, которые разбиты на пункты. В каждом разделе выполняются задачи, ведущие к достижению поставленной цели.

1 Анализ комплексной системы защиты информации ООО «ЭНЕРГО»

1.1 Описание деятельности и анализ инфраструктуры сети организации

Организация ООО «ЭНЕРГО» представляет собой негосударственное учреждение, занимающееся поставкой энергетических услуг, обработкой персональных данных клиентов и выходом на поставщиков, выдачей лицензий и другими видами деятельности. В основном в данной организации обрабатываются персональные данные клиентов. Что означает, что все персональные данные должны быть защищены должным образом в соответствии с федеральным законом №152 от 27.07.2006 г. «О персональных данных» [23, 24].

ООО «ЭНЕРГО» расположена по адресу: город Ставрополь, Прикумский переулок, д.1а.

Данная организация имеет относительно не большое число сотрудников (около 25). В скором времени ожидается расширение фирмы, увеличение видов деятельности, а также открытие филиала данной организации в городе Михайловске, при этом появляется необходимость не только модернизировать имеющуюся сеть и построить надежную распределенную вычислительную сеть, но и выбрать российское оборудование, имеющее все необходимые сертификаты ФСБ и ФСТЭК. Существующая сеть в ООО «ЭНЕРГО» поддерживается с помощью сетевого оборудования фирмы Juniper Networks. Juniper Networks – американская компания, производитель телекоммуникационного оборудования, преимущественно для интернет провайдеров, корпораций и государственного сектора [12].

С момента создания и по настоящее время, Juniper Networks специализируется на разработке скоростных решений по обработке потоковых данных для высшего уровня сетевых решений. Большинство продуктов компании использует сетевые процессоры собственной разработки и работает

под управлением JUNOS — операционной системы, основанной на FreeBSD и содержащей полный набор POSIX-совместимых команд и инструментов [12].

В сети данной организации используются около пяти единиц сетевого оборудования такие как:

− коммутаторы Juniper Networks EX3200-24T;

− маршрутизатор ADSL Zyxel AMG1302-T11C.

Маршрутизатор используется для обеспечения подключения к ресурсам сети Интернет. Коммутаторы взаимодействуют по классической иерархии «звезда». В сети выделен сервер, на котором расположены базы данных ПДн, а также базы данных бухгалтерских отчетов и программ, юридической информации. Структура сети организации, до появления филиала, и установления соединения с ним представлена на рисунке 1. В данной структуре указано разделение по отделам, которое совмещено со структурой сети организации, что дает возможность, определить какая аппаратура используется в данном отделе, и какой риск, связанный с потерей обрабатываемой информации на данном участке возможен.

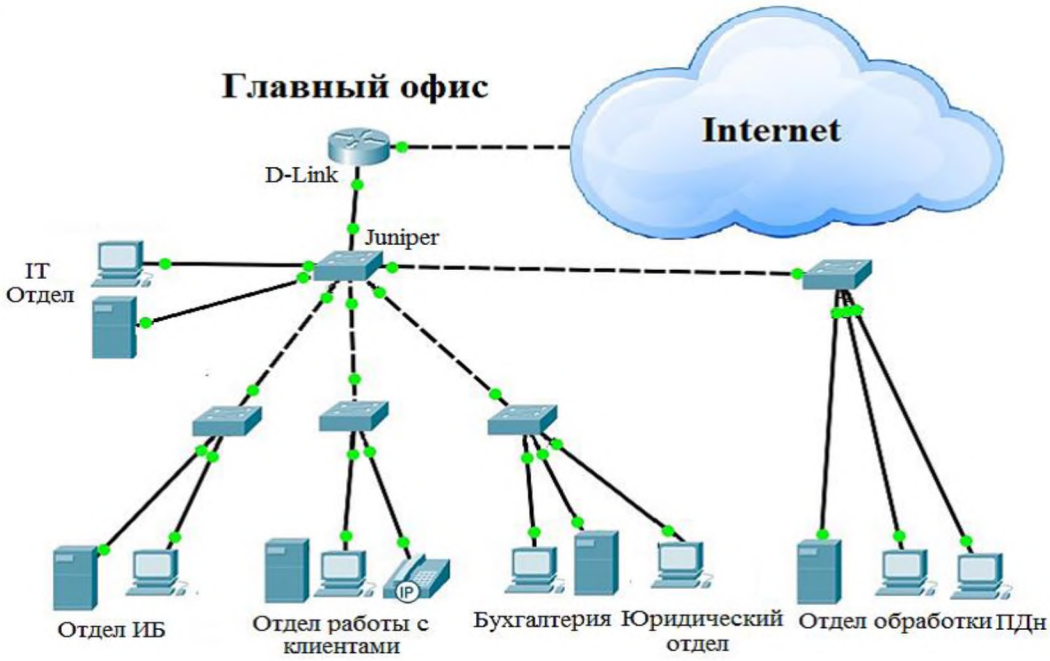

Рисунок 1 – Структура сети ООО «ЭНЕРГО»

В связи с увеличением видов деятельности организации и открытием филиала, данная структура теряет свою актуальность, и появляется

необходимость в разработке новой структуры сети, с учетом всех выявленных угроз и проблем предыдущей, а также с учетом прогнозируемых уязвимостей.

1.1.1 Анализ информационных активов ООО «ЭНЕРГО»

В данной организации большее количество информационных активов хранятся в электронном виде, и потеря данной информации представляет большой риск для организации.

Информационный актив – это информация [23]:

– с реквизитами, позволяющими её идентифицировать;

– имеющая ценность для самой организации;

– находящаяся в распоряжении и представленная на любом материальном носителе в форме, пригодной для её обработки, хранения или передачи.

В данной организации к типам информационных активов относится информация, содержащая коммерческую тайну (далее – КТ), персональные данные (ПДн) и открытую информацию.

Основные информационные активы ООО «ЭНЕРГО» хранятся в информационной системе, и так как организация после открытия филиала, стала иметь разветвленную структуру, то необходимая часть этих активов передается и циркулирует по сети. Более подробно, сведения, имеющие ценность для организации, представлены в Таблице А.1 Приложения А.

1.2 Анализ защищенности информационной системы организации от угроз информационной безопасности

Главной проблемой обеспечения защищенности конфиденциальной информации, является излишнее доверие к автоматизированным системам обработки информации (АСОИ). Помимо того, что АСОИ подвержены сбоям вследствие природных явлений, и ошибок персонала, воздействие на них могут производить и преднамеренные действия злоумышленников [6, 7].

Так как атаки на сети организаций происходили со времен появления сетей передачи данных, то за многие годы выработались правила защиты от

определенных атак. Таким образом, можно рассмотреть какие угрозы, за счет высокого уровня защиты маловероятно реализовать, а также защита от каких угроз до сих пор остаются под вопросом.

В ООО «ЭНЕРГО» защищенность информационных систем на высоком уровне. Такие угрозы как утечка информации по техническим каналам, утечка видовой информации, утечка информации по каналам ПЭМИН – маловероятны, потому что, во-первых, они, редко реализуются, а во-вторых, в данном случае защита от данных угроз находится на требуемом уровне (применяется фильтрация опасных сигналов, и правила экранирования, заземления необходимых объектов и т.д.).

Угрозы, связанные с различными природными явлениями, могут принести ощутимый ущерб организации, который постоянно выполняет множество операций и имеет базы данных с большим количеством записей. Защита от пожаров заключается в оборудовании помещений, в которых находятся элементы системы (носители цифровых данных, серверы, архивы и пр.), противопожарными датчиками, назначении ответственных за противопожарную безопасность и наличие средств пожаротушения. Всё оборудование, обрабатывающее конфиденциальную (ценную) информацию находится выше первого этажа, тем самым защищая оборудование от наводнений. Защита от молний, заключается в экранировании и заземлении сетевых кабелей, и наличии бесперебойного питания [15].

Практически все угрозы, связанные с неправомерным непосредственным доступом к информационной системе, к оборудованию организации сведены к минимуму усиленной системой охраны на входах в главные отделы организации, а также с помощью систем видеонаблюдения. Копирование на носители важных документов либо внедрение вредоносных программ трудноосуществимо за счет многоуровневой системы защиты, т.е. чтобы иметь доступ к конфиденциальной информации, нужен допуск или разрешение. Так же с помощью системы логин/пароль, выполняется аутентификация пользователей. То есть при неправомерных действиях в самой организации,

остаться не замеченным трудно. Поэтому злоумышленники уже давно пользуются сетевыми технологиями, и, с постоянным развитием и усовершенствованием средств защиты от данных угроз, так же постоянно модернизируются и способы несанкционированного проникновения [6,15].

Ранее организация имела один главный офис, но после модернизации появился филиал в городе Михайловске и, теперь, организация имеет разветвленную структуру, т.е. помимо главного офиса еще филиал, с которым в свою очередь необходимо обмениваться информацией. Самым слабым местом, в этом случае, является среда передачи данных. В ООО «ЭНЕРГО» существуют способы защиты и шифрования передаваемых данных, но они находятся на низком уровне, по сравнению с остальными средствами защиты.

Для увеличения показателей защищенности, следует выяснить, какими средствами можно минимизировать риск реализации вышеперечисленных угроз (риск информационной безопасности). В этом заключается вторая задача выпускной квалификационной работы, которая выполнена во втором разделе.

1.3 Разработка перечня актуальных угроз для организации

Под угрозами безопасности ПДн при их обработке в ИСПДн понимается совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

В общем виде все угрозы организации можно разделить на две группы: внутренние и внешние. Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая информационные активы. Внешние угрозы возникают благодаря непосредственной деятельности недобросовестных конкурентов, преступных элементов, иностранных разведывательных служб извне [6].

К числу внешних угроз относится несанкционированный доступ к информации. Несанкционированный доступ (НСД) – наиболее распространенный и многообразный вид компьютерных нарушений [6, 7]. Суть НСД состоит в получении нарушителем доступа к объекту в нарушение правил разграничения доступа, установленных в соответствии с принятой в организации политикой безопасности. НСД использует любую ошибку в системе защиты и возможен при нерациональном выборе средств защиты, их некорректной установке и настройке. НСД может быть осуществлен как штатными средствами автоматизированной системы, так и специально созданными аппаратными и программными средствами. При этом субъектом, заинтересованным в осуществлении несанкционированного доступа может оказаться государство, юридическое лицо, группа физических лиц или отдельное физическое лицо [6].

ООО «ЭНЕРГО» защищена от множества угроз. Поэтому для защиты наиболее уязвимых мест целесообразно разработать частную модель угроз, которая подробно представлена в Приложении Б, и выявить наиболее актуальные для данной организации угрозы. В таблице 1 представлена информация об актуальных угрозах ООО «ЭНЕРГО» и коэффициенте их реализуемости в организации [18].

Таблица 1 – Актуальные угрозы безопасности (Угрозы несанкционированного доступа по каналам связи) ООО «ЭНЕРГО»

№ п/п	Тип угроз безопасности	Коэффициент реализуемости угрозы
1	Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	0,75
2	Перехват за переделами контролируемой зоны	0,5
3	Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов ИСПДн, топологии сети, открытых портов и др.	0,35
4	Угрозы выявления паролей по сети	0,5
5	Угрозы навязывание ложного маршрута сети	0,75
6	Угрозы подмены доверенного объекта в сети	0,75

№ п/п	Тип угроз безопасности	Коэффициент реализуемости угрозы
7	Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,75
8	Угрозы типа «Отказ в обслуживании»	0,35
9	Угрозы удаленного запуска приложений	0,35
10	Угрозы внедрения по сети вредоносных программ	0,35

Как видно из таблицы 1, и из частной модели угроз представленной в Приложении Б, наиболее уязвимым местом является канал связи и практически все угрозы несанкционированного доступа по каналам связи плохо защищены [18]. Процентное соотношение представлено, для наглядности, в виде круговой диаграммы на рисунке 2, которая так же иллюстрирует, вероятность каких угроз превалирует среди общего количества угроз взятых для рассмотрения.

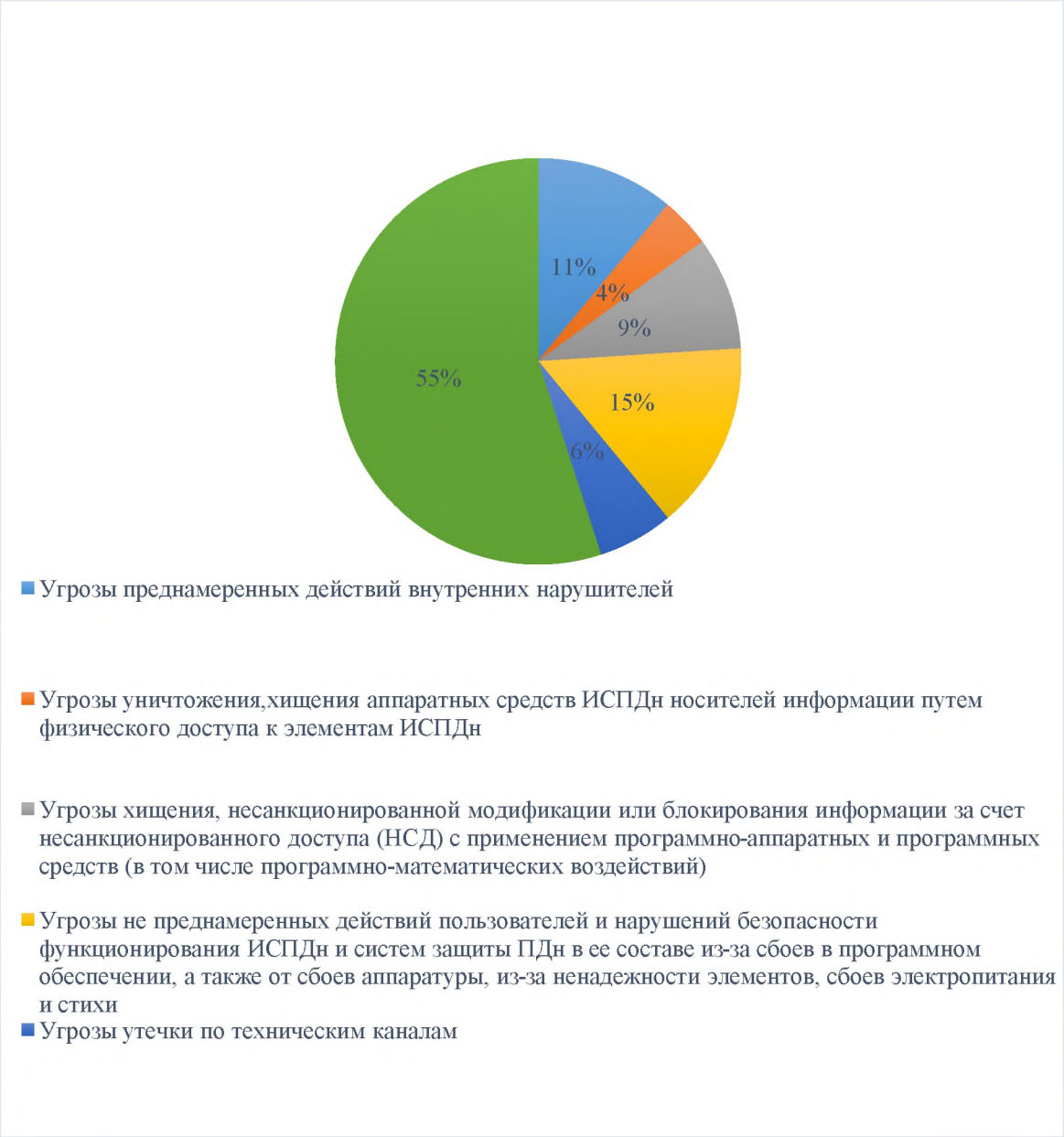

Рисунок 2 – Круговая диаграмма, иллюстрирующая процентное соотношение угроз безопасности ООО «ЭНЕРГО»

Оценка риска информационной безопасности (ИБ) проводилась по нижеприведенной формуле (1):

$$R = P_{\text{угр}} \cdot R_n \cdot C \cdot \frac{K_0 + K_t}{2} \cdot 100\%, \quad (1)$$

где: R – численная величина риска ИБ;

Pугр – вероятность реализации хотя бы одной угрозы из всего перечня угроз;

Rn – риск несоответствия требованиям законодательства;

C – ценность актива (0…1);

Ko – вероятность использования организационных уязвимостей;

Kt – вероятность использования технических уязвимостей

Проведя расчёты риска ИБ, которые более подробно представлены в Приложении Б, для типов объектов среды влияющих на качество защиты конфиденциальной информации получено [18]:

$$R = 0.99 \cdot 0.5 \cdot 0.5 \cdot \frac{0.5+0.5}{2} \cdot 100\% = 12.5\,\% \quad (2)$$

Допустимым риском принято считать риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. Для предприятий малого и среднего бизнеса рекомендованное значение риска не должно превышать 5% [18].

Рассчитанное значение значительно превышает максимальное допустимое значение риска, что означает, что существующая система защиты требует переоценки и доработки, в рамках, которые были выявлены при определении наиболее актуальных угроз.

В соответствии с выявленными угрозами, появляется определенный круг задач по повышению защищенности информации, передаваемой по каналам связи. Организация ООО «ЭНЕРГО» в большей мере подвержена внешним угрозам. Основную долю таких угроз составляют угрозы: угроза «Анализ сетевого трафика», угроза сканирования, угроза выявления паролей по сети, угроза навязывание ложного маршрута сети или объекта, угроза подмены доверенного объекта в сети. Такие угрозы реализуются при передаче данных по открытым каналам, когда трафик можно перехватить, проанализировать, а затем изменить.

Из вышесказанного следует, что в данной системе должны выполняться следующие требования [14, 16]:

– должна обеспечиваться защита информационного трафика во время прохождения открытых участков сети за пределами контролируемой зоны;

– требуется обеспечение шифрование сетевого трафика;

– требуется обеспечить защиту от несанкционированного доступа к узлам локальной сети главного офиса и филиала;

– необходимо иметь контроль доступа к сетевым устройствам.

Для построения соединения между главным офисом и филиалом, есть несколько способов, которые учитывают приведенные выше требования [17]:

– физически проложенный отдельный выделенный кабель. Он обеспечит безопасность и отличную пропускную способность канала. Это самый дорогостоящий способ;

– аренда канала у провайдера. Это достаточно распространенный вариант, так как все заботы на себя берет провайдер и ответственность за задержки и обрывы несет тоже провайдер;

– развертывание VPN внутри уже проложенной сети. Данный способ обеспечения безопасного канала передачи данных получил достаточно широкое распространение по всему миру. Этот способ является самым доступным, и наиболее применяемым в настоящее время.

Организация, использующая VPN получает заметные преимущества, заключающиеся, прежде всего, в значительной экономии финансовых средств, поскольку в этом случае компания может отказаться от построения или аренды дорогих выделенных каналов связи для создания собственных intranet/extranet сетей и использовать для этого дешевые Интернет-каналы, надежность и скорость передачи которых в большинстве своем уже не уступает выделенным линиям [13].

1.4 Выводы по разделу

В данном разделе была решена первая задача, поставленная для достижения цели выпускной квалификационной работы, а так же рассмотрены следующие вопросы:

– описана деятельности организации ООО «ЭНЕРГО»;

– проанализированы информационные активы организации;

– проанализирован уровень защищенности информационной системы от перечисленных угроз;

– выделены актуальные угрозы организации с наиболее низким уровнем защиты;

– рассчитан риск информационной безопасности.

Было выявлено, что в ООО «ЭНЕРГО» наибольшая вероятность реализации угроз присвоена тем угрозам, которые тем или иным образом связанны с передаваемой по каналам связи информацией, за счет слабой защиты. Данный факт указывает на уязвимое место в защите информации организации, и для устранения этого недостатка системы защиты нужно использовать другие, более эффективные способы защиты, которые будут представлены во втором разделе. Так же, рассчитанное значение риска ИБ значительно превышает установленную для данного показателя норму, что также является свидетельством не надежной системы защиты, и необходимости ее модернизации. После анализа защищенности и возможных угроз, были разработаны требования к методам реализации соединения и защиты данного соединения.

Выявлено, что для данной организации, целесообразно использовать технологию виртуальных частных сетей. Она позволяет развернуть одно или несколько сетевых соединений в уже существующей сети. Но необходимо учитывать что оборудование, реализующее данное соединение должно гарантировать надежную защиту, а так же быть сертифицированым.

2 Сравнительный анализ существующих методов и средств реализации VPN-технологий при построении защищенных распределенных сетей

В ходе исследований, проведённых в первом разделе, было выяснено, что безопасность информационных активов при их обработке в информационных системах обеспечивается с помощью систем защиты информации. Информационные активы обрабатываются и хранятся в информационных системах, а также передаются, с использованием определенных информационных технологий и технических средств, порождающих объекты защиты различного уровня, атаки на которые создают прямые или косвенные угрозы защищаемой информации.

В рамках поставленной в первом разделе задачи, выяснено. Что необходимо, установить защищенное соединение между главным офисом и открывающимся филиалом.

Самым распространённым в последнее время и относительно не дорогим решением является Virtual Private Network (VPN) соединение, которое позволяет организации, открывая филиалы, использовать «Интернет» в качестве среды для построения VPN, для соединения ЛВС. Удобство заключается в том, что никаких кабелей прокладывать не придется, а также, как правило, оборудование, позволяющее строить такого вида соединения, помимо этого может выполнять ряд других задач, в зависимости от комплектации и настройки оборудования. Главным вопросом при выборе определенного оборудования является «На достаточно ли высоком уровне будет защищенность информации при выборе данного продукта, и имеет ли продукт соответствующие лицензии?». Ответ на этот вопрос будет найден и обоснован в следующих двух разделах [4].

Классифицировать VPN решения можно по нескольким основным параметрам [4,12]:

По типу используемой среды:

– защищённые VPN сети. Наиболее распространённый вариант приватных частных сетей. С его помощью возможно создать надежную и защищенную подсеть на основе ненадёжной сети, как правило, Интернета. Примером защищённых VPN являются , OpenVPN и PPTP;

– доверительные VPN сети. Используются в случаях, когда передающую среду можно считать надёжной и необходимо решить лишь задачу создания виртуальной подсети в рамках большей сети. Вопросы обеспечения безопасности становятся неактуальными. Примерами подобных VPN решении являются: MPLS и L2TP. Корректнее сказать, что эти протоколы перекладывают задачу обеспечения безопасности на другие протоколы, например, такие как L2TP, который, как правило, используется в паре с IPSec.

По способу реализации:

– VPN сети в виде специального программно-аппаратного обеспечения. Реализация VPN сети осуществляется при помощи специального комплекса программно-аппаратных средств. Такая реализация обеспечивает высокую производительность и, как правило, высокую степень защищённости;

– VPN сети в виде программного решения. Используют персональный компьютер со специальным программным обеспечением, обеспечивающим функциональность VPN;

– VPN сети с интегрированным решением. Функциональность VPN обеспечивает комплекс, решающий также задачи фильтрации сетевого трафика, организации сетевого экрана и обеспечения качества обслуживания.

По назначению:

– Intranet VPN. Используют для объединения в единую защищённую сеть нескольких распределённых филиалов одной организации, обменивающихся данными по открытым каналам связи;

– Remote Access VPN. Используют для создания защищённого канала между сегментом корпоративной сети (центральным офисом или филиалом) и одиночным пользователем, который, работая дома, подключается к

корпоративным ресурсам с домашнего компьютера или, находясь в командировке, подключается к корпоративным ресурсам при помощи ноутбука.

– Extranet VPN. Используют для сетей, к которым подключаются «внешние» пользователи (например, заказчики или клиенты). Уровень доверия к ним намного ниже, чем к сотрудникам компании, поэтому требуется обеспечение специальных «рубежей» защиты, предотвращающих или ограничивающих доступ последних к особо ценной, конфиденциальной информации.

По типу протокола: Существуют реализации виртуальных частных сетей под TCP/IP, IPX и AppleTalk. Но на сегодняшний день наблюдается тенденция к всеобщему переходу на протокол TCP/IP, и абсолютное большинство VPN решений поддерживает именно его.

По уровню сетевого протокола: По уровню сетевого протокола на основе сопоставления с уровнями эталонной сетевой модели ISO/OSI.

2.1 Основные виды VPN соединений

В последнее время в мире телекоммуникаций наблюдается повышенный интерес к виртуальным частным сетям (Virtual Private Network – VPN). Это обусловлено необходимостью снижения расходов на содержание корпоративных сетей за счет более дешевого подключения удаленных офисов и удаленных пользователей через сеть Internet (рисунок 3). При сравнении стоимости услуг по соединению нескольких сетей через Internet, например, с сетями Frame Relay можно заметить существенную разницу в стоимости. Однако, стоит отметить, что при объединении сетей через сеть Интернет, сразу возникает вопрос о безопасности передаваемых данных, поэтому возникла необходимость создания механизмов, позволяющих обеспечить конфиденциальность и целостность передаваемой информации. Сети, построенные на базе таких механизмов, и получили название VPN [4, 12, 21].

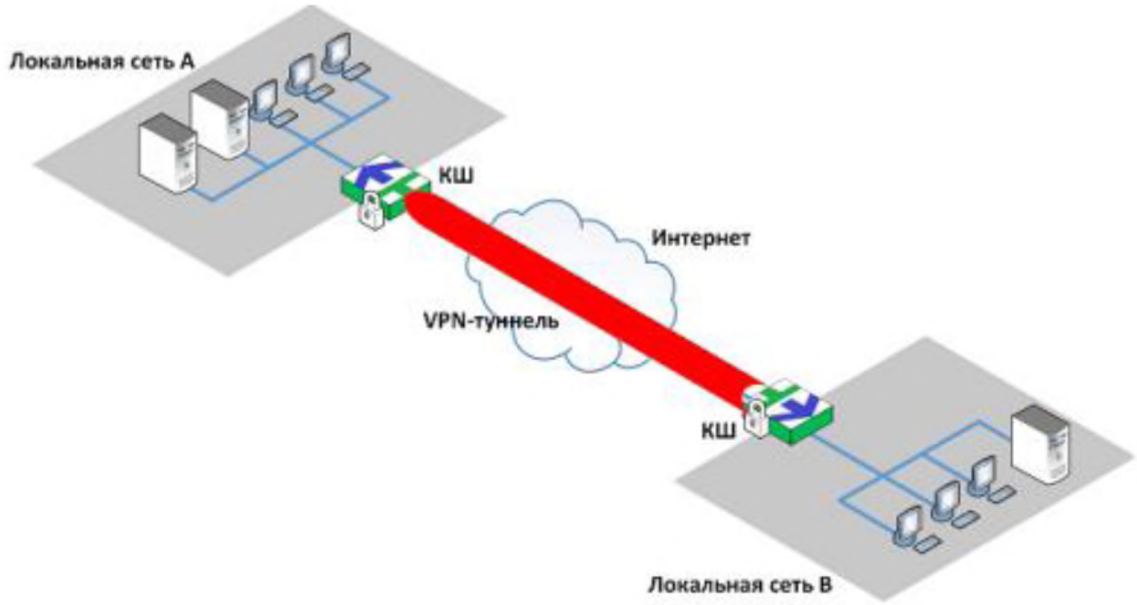

Рисунок 3 – Пример построения VPN

Структура VPN включает в себя каналы глобальной сети, защищенные протоколы и маршрутизаторы.

Для объединения удаленных локальных сетей в виртуальную сеть организации используются «виртуальные выделенные каналы». Для создания подобных соединений используется механизм туннелирования. Инициатор туннеля инкапсулирует пакеты локальной сети в новые IP-пакеты, содержащие в своем заголовке адрес инициатора туннеля и адрес конечного пользователя (терминатора) туннеля. На противоположном конце терминатором туннеля производится обратный процесс извлечения исходного пакета [12, 21].

При осуществлении такой передачи необходимо учитывать вопросы целостности и конфиденциальности данных, которые невозможно обеспечить туннелированием, без шифрования. Для достижения конфиденциальности передаваемой корпоративной информации необходимо использовать некоторый алгоритм шифрования, причем одинаковый на концах туннеля [4].

Для того чтобы была возможность создания VPN на базе оборудования и программного обеспечения от различных производителей необходим некоторый стандартный механизм. VPN могут строиться на базе различных протоколов, которые реализуют этот механизм [21]:

– VPN на базе протокола Internet Protocol Security (IPSec). IPSec описывает все стандартные методы VPN. Этот протокол определяет методы идентификации при инициализации туннеля, методы шифрования, используемые конечными точками туннеля и механизмы обмена и управления ключами шифрования между этими точками. Из недостатков этого протокола можно отметить то, что он ориентирован на IP. Протокол IPSec тесно связан с протоколом IKE (Internet Key Exchange), позволяющем обеспечить передачу информации по туннелю, и решить задачи безопасного управления и обмена криптографическими ключами между удаленными устройствами, в то время, как IPSec кодирует и подписывает пакеты;

– VPN на базе протокола (Point-to-Point Tunneling Protocol) PPTP. Туннельный протокол типа точка-точка, позволяющий компьютеру устанавливать защищённое соединение с сервером за счёт создания специального туннеля в стандартной, незащищённой сети. PPTP помещает (инкапсулирует) кадры PPP в IP-пакеты для передачи по глобальной IP-сети, например Интернет. Протокол считается менее безопасным, чем IPSec. PPTP работает, устанавливая обычную PPP сессию с противоположной стороной с помощью протокола Generic Routing Encapsulation. Второе соединение на TCP-порту 1723 используется для инициации и управления GRE-соединением. PPTP сложно перенаправлять за сетевой экран, так как он требует одновременного установления двух сетевых сессий [21];

– VPN на базе протокола OpenVPN. OpenVPN - свободная реализация технологии виртуальной частной сети (VPN) с открытым исходным кодом для создания зашифрованных каналов типа точка-точка или сервер-клиенты между компьютерами. Она позволяет устанавливать соединения между компьютерами, находящимися за NAT и сетевым экраном, без необходимости изменения их настроек. Для обеспечения безопасности управляющего канала и потока данных OpenVPN использует библиотеку OpenSSL. OpenVPN проводит все сетевые операции через TCP или UDP транспорт;

– VPN на базе протокола (Layer 2 Tunneling Protocol) L2TP. Протокол туннелирования второго уровня используется для поддержки виртуальных частных сетей. Главное достоинство L2TP состоит в том, что этот протокол позволяет создавать туннель не только в сетях IP, но и в таких, как ATM, X.25 и Frame Relay [12,21, 25].

2.2 Оборудование, реализующее VPN соединение

Существуют различные варианты построения VPN. При выборе решения требуется учитывать факторы производительности средств построения VPN. Например, если маршрутизатор и так работает на пределе мощности своего процессора, то добавление туннелей VPN и применение шифрования или дешифрования информации могут остановить работу всей сети из-за того, что этот маршрутизатор не будет справляться с трафиком, не говоря уже о VPN.

Для построения VPN лучше всего использовать специализированное оборудование, однако если имеется ограничение в средствах, то можно обратить внимание на программное решение [21, 25].

2.2.1 Виртуальная частная сеть на базе межсетевых экранов

Межсетевые экраны большинства производителей поддерживают туннелирование и шифрование данных. Все подобные продукты основаны на том, что если трафик проходит через межсетевой экран, то можно его и зашифровать. К программному обеспечению собственно межсетевого экрана добавляется модуль шифрования. Недостатком данного метода можно назвать зависимость производительности от аппаратного обеспечения, на котором работает межсетевой экран. При использовании межсетевых экранов на базе персональных компьютеров (ПК) надо помнить, что подобное решение можно применять только для небольших сетей с небольшим объемом передаваемой информации [21, 26].

2.2.2 Виртуальная частная сеть на базе маршрутизаторов

Другим способом построения VPN является применение для создания защищенных каналов маршрутизаторов. Так как вся информация, исходящая из

локальной сети, проходит через маршрутизатор, то целесообразно возложить на этот маршрутизатор и задачи шифрования [21, 25].

Примером оборудования для построения VPN на маршрутизаторах является оборудование компании Cisco Systems. Начиная с версии программного обеспечения IOS 11.3(3)T маршрутизаторы Cisco поддерживают протоколы L2TP и IPSec. Помимо простого шифрования проходящей информации Cisco поддерживает и другие функции VPN, такие как идентификация при установлении туннельного соединения и обмен ключами [3,4].

2.2.3 Виртуальная частная сеть на базе программного обеспечения

Следующим подходом к построению VPN являются чисто программные решения. При реализации такого решения используется специализированное программное обеспечение, которое работает на выделенном компьютере и в большинстве случаев выполняет роль proxy-сервера. Компьютер с таким программным обеспечением может быть расположен за межсетевым экраном [9,21].

В качестве примера такого решения можно выступает программное обеспечение AltaVista Tunnel 97 компании Digital. При использовании данного ПО клиент подключается к серверу Tunnel 97, аутентифицируется на нем и обменивается ключами. Шифрация производится на базе 56 или 128 битных ключей Rivest-Cipher 4, полученных в процессе установления соединения. Далее, зашифрованные пакеты инкапсулируются в другие IP-пакеты, которые в свою очередь отправляются на сервер. В ходе работы Tunnel 97 осуществляет проверку целостности данных по алгоритму MD5. Кроме того, данное ПО каждые 30 минут генерирует новые ключи, что значительно повышает защищенность соединения [18 – 21].

2.2.4 Виртуальная частная сеть на базе сетевой ОС

Решения на базе сетевой операционной системы (ОС) рассмотрены на примере системы Windows NT компании Microsoft. Для создания VPN Microsoft использует протокол PPTP, который интегрирован в систему Windows NT.

Данное решение очень привлекательно для организаций, использующих Windows в качестве корпоративной операционной системы. Необходимо отметить, что стоимость такого решения значительно ниже стоимости прочих решений. В работе VPN на базе Windows NT используется база пользователей NT, хранящаяся на Primary Domain Controller (PDC). При подключении к PPTP-серверу пользователь аутентифицируется по протоколам PAP, CHAP или MS-CHAP. Передаваемые пакеты инкапсулируются в пакеты GRE/PPTP. Для шифрования пакетов используется нестандартный протокол от Microsoft Point-to-Point Encryption с 40 или 128 битным ключом, получаемым в момент установки соединения [12, 21]

2.2.5 Виртуальная частная сеть на базе аппаратных средств

Вариант построения VPN на специальных устройствах может быть использован в сетях, требующих высокой производительности. Примером такого решения служит продукт cIPro-VPN компании Radguard

Данный продукт использует аппаратное шифрование передаваемой информации, способное пропускать поток в 100 Мбит/с. cIPro-VPN поддерживает протокол IPSec и механизм управления ключами ISAKMP/Oakley. Помимо прочего, данное устройство поддерживает средства трансляции сетевых адресов и может быть дополнено специальной платой, добавляющей функции межсетевого экрана [19, 21].

Сравнительный анализ приведенных выше методов и средств реализации VPN соединения приведен в таблице 2.

Таблица 2 – Сравнительный анализ методов реализации VPN соединения

Метод	Достоинства	Недостатки
VPN на базе межсетевых экранов	Легкость реализации.	Производительность напрямую зависит от аппаратного обеспечения.
	Комплексность обработки.	Ограниченность в функциях
VPN на базе маршрутизаторов	Легкость реализации	Высокая стоимость
	Многофункциональность	

Метод	Достоинства	Недостатки
	Высокая производительность	Необходимость дополнительной защиты
	Возможность усовершенствования	
VPN на базе программного обеспечения	Низкая стоимость	Нестандартная архитектура
	Простота установки	Низкая производительность
	Легкость управления	
VPN на базе сетевой ОС	Легкость интеграции с Windows и другими ОС	Отсутствие проверки целостности данных;
	Низкая стоимость	Невозможность смены ключей во время соединения.
		Необходимость дополнительной защиты
VPN на базе аппаратных средств	Высокая производительность;	Высокая стоимость
	Возможность модульного усовершенствования.	Не универсальность

Исходя из проведенного анализа, можно сказать, что каждый метод имеет свои достоинства и недостатки. Для ООО «ЭНЕРГО», будет выбран комбинированный метод, а именно аппаратно-программный комплекс, что позволит увеличить число достоинств и снизить количество недостатков. При этом, так как в организации обрабатываются персональные данные, а также информация, связанная с лицензированием, средство должно быть отечественным продуктом, имеющим сертификаты ФСБ и ФСТЭК [1].

2.3 Реализация VPN соединений в АПКШ «Континент»

Для установления защищенного соединения с помощью VPN между главным офисом ООО «ЭНЕРГО» и его филиалом, выбран аппаратно-программный комплекс «Континент», так как он является лидером рынка сертифицированных VPN-шлюзов для защиты сети организации. Характеристики других, похожих средств защиты представлены в Приложении Г. На основе их анализа, выбран самый приемлемый вариант – комплекс «Континент». Использование данного комплекса поможет уменьшить количество угроз, реализуемых с большой вероятностью, и тем самым,

повысить уровень защищенности сети организации. Так же в версии 3.7 устранены проблемы, встречающиеся в предыдущих версиях, что открывает множество возможностей для обеспечения защиты [5, 10, 22, 25].

«Континент» – семейство продуктов для обеспечения сетевой безопасности при подключении к сетям общего пользования посредством межсетевого экранирования, построения частных виртуальных сетей (VPN) и системы обнаружения вторжений (СОВ) [10].

Комплекс обеспечивает криптографическую защиту информации (в соответствии с ГОСТ 28147–89), передаваемой по открытым каналам связи, между составными частями VPN, которыми могут являться локальные вычислительные сети, их сегменты и отдельные компьютеры. Благодаря использованию данного алгоритма, возможность реализации атаки на криптографические ключи мала, так как длина ключа в данном алгоритме составляет 256 бит [2, 8. 10].

Современная ключевая схема, реализуя шифрование каждого пакета на уникальном ключе, обеспечивает гарантированную защиту от возможности дешифрации перехваченных данных [2, 8].

Для защиты от проникновения со стороны сетей общего пользования комплекс «Континент» обеспечивает фильтрацию принимаемых и передаваемых пакетов по различным критериям (адресам отправителя и получателя, протоколам, номерам портов, дополнительным полям пакетов и т.д.). Осуществляет поддержку VoIP, видеоконференций, ADSL, Dial-Up и спутниковых каналов связи, технологии NAT/PAT для сокрытия структуры сети [10, 19].

Область применения продуктов «Континент» [10]:

– защита внешнего периметра сети от вредоносного воздействия со стороны сетей общего пользования;

– создание отказоустойчивой VPN-сети между территориально распределенными сетями;

– защита сетевого трафика в мультисервисных сетях (VoIP, Video conference);

– разделение сети на сегменты с различным уровнем доступа;

– организация защищенного удаленного доступа к сети для мобильных сотрудников;

– защита беспроводных сегментов сетей;

– организация защищенного межсетевого взаимодействия между конфиденциальными сетями.

2.3.1 Возможности АПКШ «Континент».

Основными возможностями данного аппаратно-программного продукта являются [10]:

– эффективная защита корпоративных сетей, и безопасный доступ пользователей VPN к ресурсам сетей общего пользования;

– криптографическая защита передаваемых данных в соответствии с ГОСТ 28147–89. В АПКШ «Континент» применяется современная ключевая схема, реализующая шифрование каждого пакета на уникальном ключе. Это обеспечивает высокую степень защиты данных от расшифровки в случае их перехвата. Шифрование данных производится в режиме гаммирования с обратной связью [2, 8];

– межсетевое экранирование – защита внутренних сегментов сети от несанкционированного доступа. Криптошлюз «Континент» обеспечивает фильтрацию принимаемых и передаваемых пакетов по различным критериям. Это позволяет защитить внутренние сегменты сети от проникновения из сетей общего пользования;

– безопасный доступ удаленных пользователей к ресурсам VPN-сети. Специальное программное обеспечение «Континент АП», входящее в состав АПКШ «Континент», позволяет организовать защищенный доступ с удаленных компьютеров к корпоративной VPN-сети;

– создание информационных подсистем с разделением доступа на физическом уровне. В АПКШ «Континент» версии 3.7 можно подключать 1

внешний и от 3 до 9 внутренних интерфейсов на каждом криптошлюзе. Это значительно расширяет возможности пользователя при настройке сети в соответствии с корпоративной политикой безопасности;

– возможность идентификации и аутентификации пользователей, работающих на компьютерах в защищаемой сети криптошлюзов. Идентификация и аутентификация пользователей выполняются с помощью специальной программы «Клиент аутентификации пользователя», установленной на компьютере пользователя защищенной сети.

2.3.2 Основные характеристики АПКШ «Континент»

Характеристики, присущие данному комплексу[10,19]:

– поддержка распространенных каналов связи. Работа через Dial-Up соединения, оборудование ADSL, подключенное непосредственно к криптошлюзу, а также через спутниковые каналы связи;

– прозрачность для любых приложений и сетевых сервисов;

– работа с высокоприоритетным трафиком. Реализованный в АПКШ «Континент» 3.7 механизм приоритизации трафика позволяет защищать голосовой (VoIP) трафик и видеоконференции без потери качества связи;

– резервирование гарантированной полосы пропускания за определенными сервисами;

– поддержка VLAN. Поддержка VLAN гарантирует простое встраивание АПКШ в сетевую инфраструктуру, разбитую на виртуальные сегменты;

– скрытие внутренней сети. Поддержка технологий NAT/PAT. Поддержка технологии NAT/PAT позволяет скрывать внутреннюю структуру защищаемых сегментов сети при передаче открытого трафика, а также организовывать демилитаризованные зоны и сегментировать защищаемые сети;

– NAT внутри VPN-связей. Реализован механизм виртуальной адресации для обеспечения возможности обмена информацией между защищаемыми IP-подсетями с пересекающимся или одинаковым адресным пространством;

– интеграция с внешними системами анализа событий безопасности. В состав АПКШ «Континент» входит модуль «ArcSight коннектор», предназначенный для выгрузки событий в систему ArcSight ESM;

– L2VPN.Дополнительный модуль ПАК «Криптографический коммутатор» обеспечивает поддержку режима L2VPN для объединения распределенных сетей на канальном уровне L2 без изменения адресного пространства;

– поддержка NTP на ЦУСе. Возможность автоматической синхронизации времени ЦУС и всей сети криптошлюзов с заданным сервером точного времени по протоколу NTP;

– АРМ генерации ключей. В состав комплекса добавлено автоматизированное рабочее место генерации ключей для введения режима управления по схеме трехлетнего хранения ключевой информации;

– поддержка протокола IPv6. Реализована поддержка работы с каналами связи, использующими протокол IPv6;

– режим повышенной безопасности. Позволяет создавать группы криптографических шлюзов с политиками безопасности, исключающими попадание незашифрованного трафика во внешние сети;

– возможность удобного защищенного взаимодействия между сетями разных организаций. Обеспечивается возможность установления доверительных отношений между криптошлюзами, принадлежащими разным криптографическим сетям и управляемыми разными ЦУС, для организации защищенного обмена между разными организациями;

– возможность интеграции с системами обнаружения атак. На каждом криптошлюзе существует возможность специально выделить один из интерфейсов для проверки трафика, проходящего через КШ, на наличие попыток неавторизованного доступа (сетевых атак). Для этого необходимо определить такой интерфейс, как «SPAN-порт», и подключить к нему компьютер с установленной системой обнаружения атак (например RealSecure).

После этого на данный интерфейс начинают ретранслироваться все пакеты, поступающие на вход пакетного фильтра криптошлюза;

– защита от DoS-атак типа SYN-flood. Для защиты от DoS-атак предусмотрен механизм антиспуфинга. Специальные механизмы борьбы с SYN-flood позволяют либо ограничить количество соединений, используя «агента» (TCP proxy), либо блокировать соединение до целевого сервера до тех пор, пока клиент не ответит на свой собственный запрос подтверждением в рамках стандартного алгоритма работы TCP. Полуоткрытые соединения с просроченным временем ожидания автоматически удаляются из таблицы состояния;

– поддержка внешних 3G-модемов (USB). Реализована поддержка внешних 3G-модемов (USB) для подключения криптошлюзов через провайдеров сотовых сетей;

– функционал DHCP сервера на КШ. Позволяет назначать динамические IP адреса клиентским устройствам, DHCP relay.

2.3.3 Обслуживание и управление АПКШ «Континент»

Управление и обслуживание элементов сети АПКШ «Континент» на высоком уровне[10]:

– удобство и простота обслуживания (необслуживаемый режим 24*7). АПКШ «Континент» 3.7 не требует постоянного локального администрирования и может работать в необслуживаемом режиме 24*7x365;

– удаленное обновление ПО криптошлюзов. В комплексе решена проблема обновления программного обеспечения криптошлюзов в территориально распределенных системах. Обновление ПО загружается в комплекс централизованно, рассылается на все криптошлюзы, входящие в состав комплекса, и автоматически устанавливается;

– обеспечение отказоустойчивости. Аппаратное резервирование криптографических шлюзов (создание кластера высокого доступа). В случае выхода из строя одного из криптошлюзов переключение на резервный

производится автоматически без вмешательства администратора и без разрыва установленных соединений;

– централизованное управление сетью;

– ролевое управление – разделение полномочий на администрирование комплекса. Реализована возможность разделения полномочий на администрирование комплекса, например, на управление ключевой информацией;

– взаимодействие с системами управления сетью. Позволяет контролировать состояние АПКШ «Континент» 3.7 по протоколу SNMPv2 из систем глобального управления сетью (Hewlett-Packard, Cisco и др.);

– локальный контроль работы криптошлюзов.

2.4 Выводы по разделу

В данном разделе была решена вторая задача, поставленная для достижения цели выпускной квалификационной работы, а также рассмотрены следующие вопросы:

– описаны возможности VPN туннелирования;

– произведен сравнительный анализ оборудования, за счет которого можно организовать VPN туннелирование;

– описан выбранный для дальнейшего исследования, и защиты распределенной сети организации, АПКШ «Континент».

Проанализировав все возможные варианты построения виртуальных частных сетей можно сделать вывод, что построение на базе комбинированного решения, то есть на базе аппаратно-программного комплекса, будет наиболее выгодным вариантом.

Недостаток его высокой стоимости, легко компенсируется за счет многообразия выполняемых функций комплекса, и гарантированной защиты путем шифрования, наличие сертификатов так же является признаком его качественности.

3 Рекомендации по построению защищенной распределенной сети организации на базе сети Интернет с использованием АПКШ «Континент»

В предыдущем разделе сделан вывод о целесообразности построения VPN соединения на оборудовании «Континент» для обеспечения двустороннего соединения между филиалом и головным офисом.

После установки и коммутации сетевого оборудования можно приступить к дальнейшей настройке.

3.1 Общие рекомендации по установке и настройке программного обеспечения и оборудования «Континент»

Первым шагом в обеспечении надежного уровня защищенности, в любой организации или на предприятии, имеющем конфиденциальную информацию, необходимо отделить вычислительную технику обрабатывающую персональные данные, от вычислительной техники, обрабатывающей только открытую информацию, и поместить ее в отдельное помещение(ия), в соответствии с типом обрабатываемых данных[5,7,9,25].

Во-вторых, установить аппаратно-программный модуль доверенной загрузки «Соболь», на компьютеры, обрабатывающие ПДн. Электронный замок «Соболь» может быть использован для того, чтобы доступ к информации на компьютере получили только те сотрудники, которые имеют на это право, и кроме этого, в случае повреждения операционной системы или важных информационных массивов, хранящихся на компьютере, администратор мог вовремя принять меры по восстановлению информации. Он не только вполне совместим с АПКШ «Континент», но и дополняет его функциональные возможности, до максимальной гарантии защищённости информации, при этом он также имеет сертификаты ФСТЭК и ФСБ. Идентификация пользователей может проходить по любым типам идентификаторов [10].

Перечень минимального необходимого оборудования представлен в таблице В.1 Приложения В.

Связь между данными локальной вычислительной сети осуществляется по каналам связи общих сетей передачи данных. К общим сетям локальная вычислительная сеть должна быть подключена через криптографический шлюз. Подключение локальной вычислительной сети через криптографический шлюз обеспечивает скрытие внутренней структуры защищаемого сегмента сети. При этом IP-адреса компьютеров в защищаемых сегментах должны быть уникальными только в рамках данной корпоративной сети [4,7, 13, 19].

Криптографический шлюз может содержать несколько сетевых интерфейсов, к которым можно подключить несколько независимых локальных сетей. При подключении компьютеров к криптографическому шлюзу может осуществляться их аутентификация. Предусмотрена поддержка виртуальных локальных сетей (VLAN), организованных в защищенных сегментах сети [10, 13].

Для обеспечения надежной защиты, компьютеры, обрабатывающие КТ и ПДн стоит объединить в разные виртуальные локальные сети, без возможности общаться друг с другом, либо с определенными правилами, которые устанавливаются, при настройке криптографического шлюза [6].

Для гарантии защищенности данных, нужно сделать, так чтобы выход в сеть Интернет был только с компьютеров обрабатывающих открытую информацию.

Таким образом, на компьютеры, на которых обрабатывается ПДн, нужно установить программное обеспечение комплекса «Соболь» (программа управления шаблонами, утилита CreateFiles), и подключить его аппаратную часть.

Установка выполняется лицом, имеющим права локального администратора на данном компьютере. Для установки необходимо завершить работу всех приложений, выполняющихся на компьютере, отключить или приостановить работу антивирусных программ [7, 10].

Далее следует установить и настроить криптопровайдер КриптоПро CSP (в случае если указанное ПО не установлено). Процедуры установки и

настройки подробно рассматриваются в эксплуатационной документации на данный программный продукт.

После установки КриптоПро нужно установить программное обеспечение Абонентского пункта (АП) для этого следует запустить на исполнение файл setup.exe, находящийся в каталоге с дистрибутивом АП и выполнить установку.

3.1.1 Защищенное управление маршрутизатором, размещенным после криптографического шлюза

При отсутствии прямого доступа к каналу (сети) передачи данных предусмотрена возможность подключения криптографического шлюза к телефонной коммутируемой или выделенной линии с помощью модема. Криптографический шлюз (КШ) осуществляет маршрутизацию проходящего через него трафика IP-пакетов, поэтому дополнительный маршрутизатор в общем случае не требуется [10, 13, 19].

При необходимости использования дополнительного маршрутизатора, его можно разместить как перед криптографическим шлюзом (в защищаемом сегменте сети), так и после (вне защищаемого сегмента сети). Если маршрутизатор находится в защищаемом сегменте сети, дополнительных действий по защите маршрутизатора не требуется. Если маршрутизатор находится вне защищаемого сегмента сети, то предусмотрена возможность защищенного управления маршрутизатором [10].

Защищенное управление маршрутизатором, размещенным после криптографического шлюза изображено на рисунке 4.

Рисунок 4 – Защищенное управление маршрутизатором, размещенным после криптографического шлюза

– на криптографическом шлюзе КШ 2 следует определить защищенную сеть из одного маршрутизатора;

– на криптографических шлюзах КШ 1 и КШ 2 нужно создать правила фильтрации, разрешающие прохождение управляющего трафика;

– на маршрутизаторе нужно добавить правило маршрутизации для отсылки IP-пакетов к консоли управления через криптографический шлюз КШ2.

3.1.2 Защита сети организации с использованием в комплексе более пяти криптографических шлюзов

Кроме маршрутизации трафика криптографический шлюз осуществляет обработку входящих и исходящих IP-пакетов: фильтрацию и криптографическое преобразование данных, передаваемых по общим каналам связи [5, 24].

Для организации доступа пользователей корпоративной сети к узлам общей сети используется механизм трансляции сетевых адресов (Network Address Translation — NAT). Автоматическое управление криптографическими шлюзами осуществляет центр управления сетью (ЦУС), размещающийся на одном из криптографических шлюзов. Этот криптографический шлюз можно

использовать как любой другой рядовой шлюз в корпоративной сети для приема и передачи IP-пакетов, их фильтрации, маршрутизации и криптографического преобразования [19, 25].

Руководство администратора «Администратор комплекса» управляет криптографическими шлюзами через ЦУС с помощью программы управления. Программа управления устанавливается на выделенном компьютере, входящем в состав защищаемого сегмента корпоративной сети (АРМ управления сетью КШ). Но данный вариант использования комплекса применим только для небольших сетей (2–5 КШ). При использовании в комплексе более пяти криптографических шлюзов рекомендуется ЦУС и АРМ управления сетью КШ вынести в отдельный защищаемый сегмент (Рисунок 5). В этом случае ЦУС используется только для управления сетью КШ [10, 26].

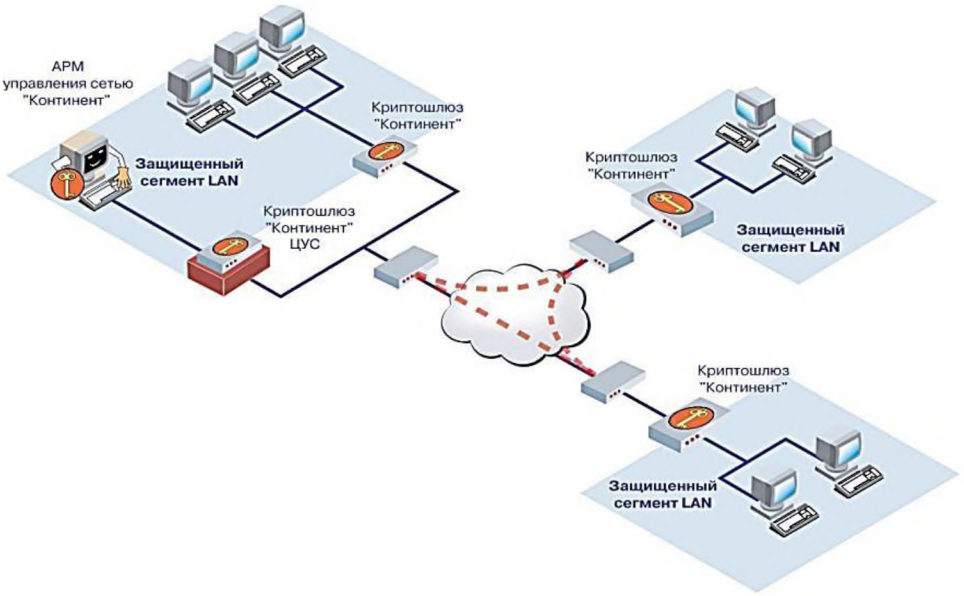

Рисунок 5 – Защита сети организации с использованием в комплексе более пяти криптографических шлюзов

Если на пути зашифрованного трафика находятся межсетевые экраны или другое оборудование, осуществляющее фильтрацию IP-пакетов, необходимо создать для них правила, разрешающие прохождение служебных пакетов комплекса [4].

Если криптографический шлюз, поддерживает трансляцию сетевых адресов (NAT), то нужно учесть, что на пути трафика между двумя КШ не

должно быть более одного сетевого устройства с поддержкой динамической трансляции адресов. Криптографический шлюз, на который установлен ЦУС, должен всегда иметь публичный адрес.

Администратор может сформировать правила фильтрации для разрешения незашифрованных соединений со сторонними абонентами. При разрешении нешифрованных соединений общий уровень защищенности корпоративной сети снижается, поэтому для обеспечения максимального уровня защиты информации рекомендуется отказаться от разрешения таких соединений [4-6,9].

Для правила фильтрации, разрешающего TCP-соединение, можно включить режим защиты от DoS-атак типа SYN-флуд. Для этого используют следующие параметры [10, 19]:

– максимальное количество соединений, которое может быть установлено по указанному правилу фильтрации;

– время, по истечении которого неактивное соединение будет автоматически разорвано;

– количество новых соединений, регистрируемых для данного правила, в секунду.

Для проверки всего трафика, проходящего через КШ, на наличие попыток неавторизованного доступа (сетевых атак) к одному из сетевых интерфейсов КШ подключают выделенный компьютер с установленной на нем системой обнаружения атак, и этот интерфейс определяется как SPAN-порт (Switched Port Analyzer). Через этот порт система обнаружения атак получает копии всех IP-пакетов, проходящих через КШ, и анализирует их на наличие неавторизованных или подозрительных действий. Копии IP-пакетов, отправляемых или поступивших по защищенному каналу, передаются на SPAN-порт соответственно до их зашифровывания или после расшифровывания [4, 7].

Также можно настроить аутентификацию пользователей, установив программу «Клиент аутентификации пользователя», а так же включить на КШ режим «Аутентификация пользователей».

Для сохранности введенных настроек рекомендуется после очередного изменения настроек комплекса сохранять резервную копию вручную.

Сотрудники, выполняющие развертывание комплекса, должны быть квалифицированными специалистами по обслуживанию вычислительной техники и иметь навыки настройки оборудования для работы в локальной сети[6].

3.1.3 Рекомендации по построению защищенной распределенной сети организации с использованием АПКШ «Континент»

Модернизированная распределенная сеть организации, представлена на рисунке 6. Канал связи между главным офисом и филиалом представляет собой VPN туннель, который обеспечивает высокий уровень защищенности передаваемых данных. Кроме того, установка криптошлюзов «Континент» позволяет не только выполнять обычную маршрутизацию, но и выполнять шифрование сетевого трафика, противостоять атакам «Анализ трафика», «Отказ в обслуживании», DoS атаке и многим другим. Данное оборудование предусматривает межсетевое экранирование, что дает данному комплексу очевидные преимущества, не смотря на немного завышенную цену на продукты данного семейства, цена во многом оправдывает себя [10].

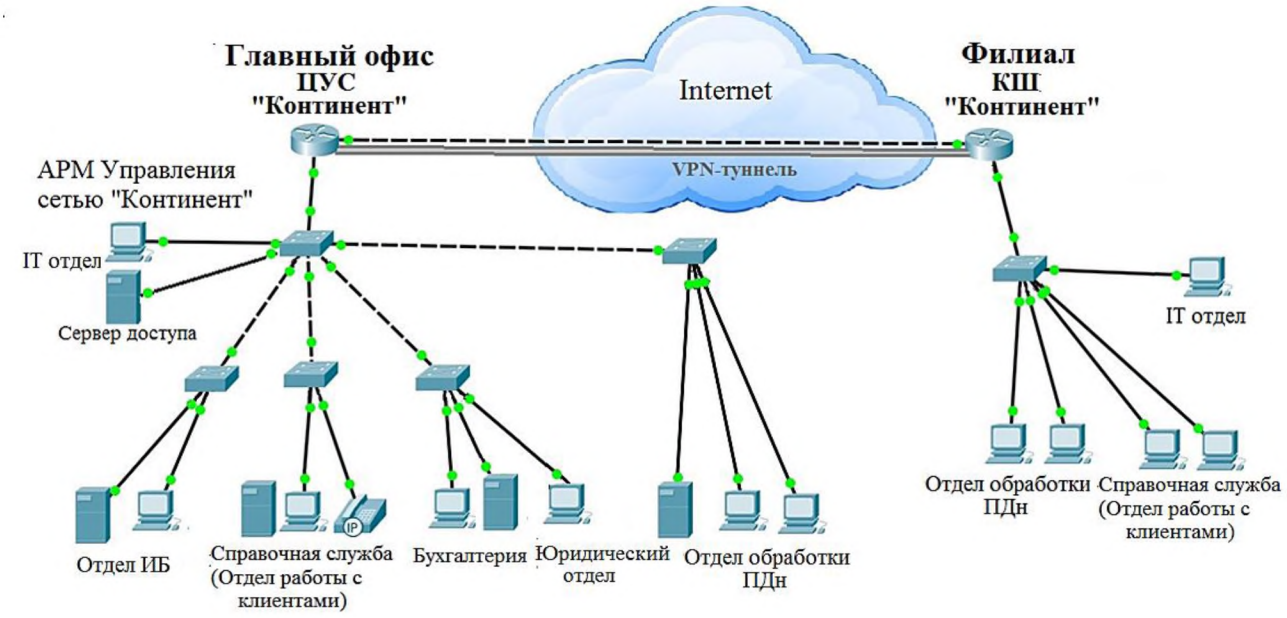

Рисунок 6 – Модернизированная сеть ООО «ЭНЕРГО»

Существующая сеть организации незначительно изменена, внутрисетевое оборудование осталось прежним. Маршрутизаторы главного офиса и филиала заменены на оборудование «Континент», Криптографический шлюз с установленной на нем программой центрального управления сетью «Континент» и Криптошлюз «Континент» соответственно, необходимое для построения защищенного соединения (Site-to-site VPN туннеля). Сеть филиала, так же осталась без изменений, кроме замены маршрутизатора. Помимо этих изменений в сети главного офиса, в силу необходимости, в IT отделе находится сервер доступа, а так же АРМ Управления сетью «Континент» [10].

Для данной организации, в силу того, что оно имеет филиал и множество рабочих мест, будет использоваться криптографический шлюз «Континент» IPC-100, так как он может записывать до 500 записей в таблице состояния соединений. Внешний вид с описанием его портов и индикаторов представлен на рисунке 7.

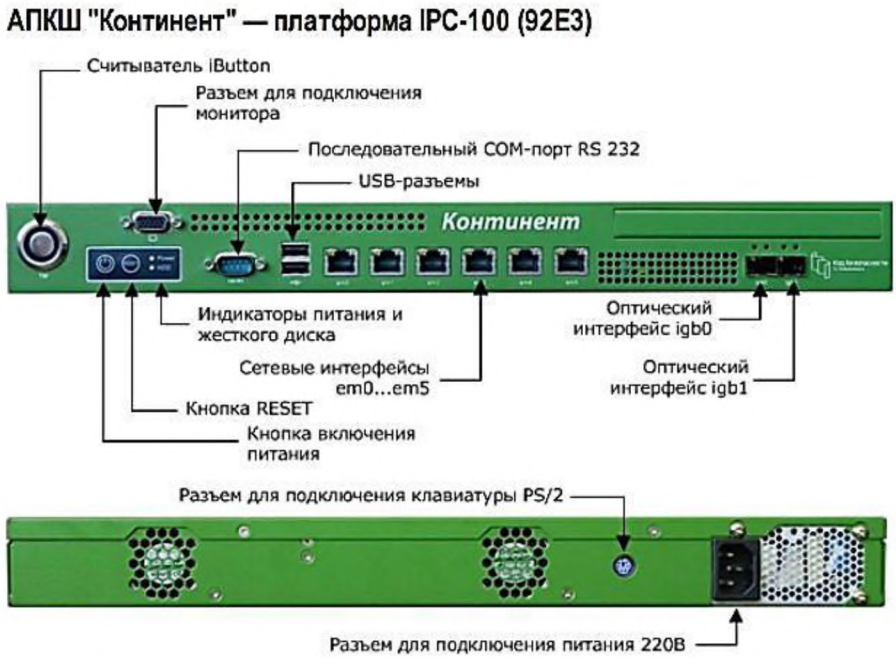

Рисунок 7 – Внешний вид криптошлюза «Континент» IPC-100

На компьютер АРМ Управления сетью необходимо установить АРМ администратора, специальную программу управления (ПУ) криптошлюзами, а так же программу управления сервером доступа, т.е. программу управления ключами. А так же программно-аппаратный комплекс (ПАК) Соболь и программное обеспечение КриптоПро. После этого выполнить базовую настройку криптошлюзов, настройку их адресов, и правил фильтрации.

Помимо лицензированной операционной системы Windows 2008 Server x64, на АРМ Главного офиса и филиала необходимо установить дополнительное ПО: СКЗИ «КриптоПро CSP 3.6 R2/3.6.1»; ПАК «Соболь 3.0»; версии систем управления базами данных для хранения журналов; MSSQL 2008 Server x32/x64; Oracle 11g x32; MS Internet Explorer 6.0 и выше.

3.3 Рекомендации по настройке защищенного VPN соединения между главным офисом и филиалом

Криптошлюзы «Континент» 3.7 имеют операционную систему Continent OS – это усовершенствованная ОС с усиленной безопасностью на основе ядра FreeBSD. Данная система, практически не дает обычному пользователю работать в режиме командной строки, вся настройка основывается на работе в

диалоговых окнах, т.к. пользовательский интерфейс – GUI (Graphic Users Interface) графический интерфейс пользователя. Поэтому дальнейшие рекомендации, имеют вид некоего алгоритма действий, нежели списка команд [10, 24]. Схема сети организации, с IP адресами, изображена на рис. 8.

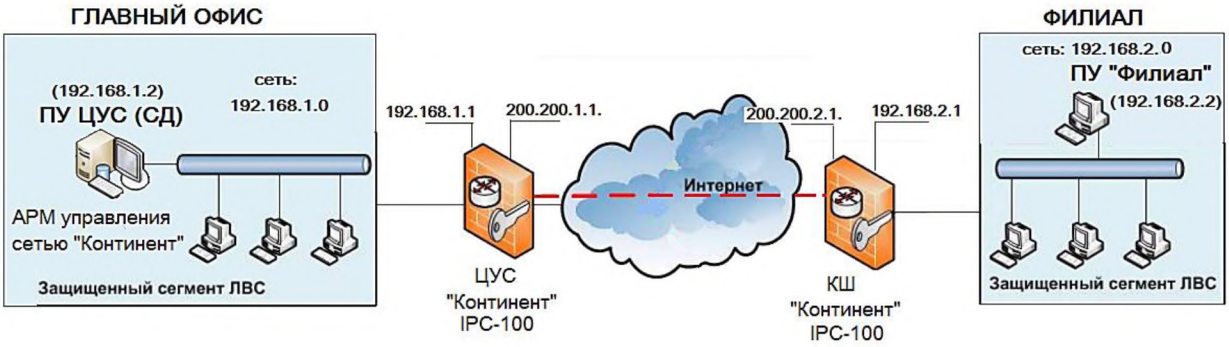

Рисунок 8 – Условная схема расположения сетевого оборудования «Континент»

3.3.1 Настройка криптографического шлюза и сохранение конфигурации

Регистрация криптографических шлюзов осуществляется с помощью Программы управления после установки соединения с ЦУС и появления на экране основного окна этой программы[10].

Для этого необходимо вызвать меню «Объекты» и в подменю «Создать» активировать команду «Криптошлюз...», либо, нажав правой кнопкой мыши на объекте «Криптошлюзы» выбрать команду «Создать криптошлюз...»

На экране появится стартовый диалог создания криптографического шлюза. В поле «Название» нужно написать название криптошлюза – FILIAL_ORG. В поле «Описание» можно написать описание данного криптошлюза, можно оставить пустым. В строке конфигурации, необходимо написать конфигурацию для данной настройки филиала, в данном случае она может иметь вид: 0000000231e0*000Dle1*000Dle2*000Dle3*000Dffff. (Пример конфигурационного файла представлен на рисунке 9.)

Далее необходимо установить часовой пояс, в котором установлен криптошлюз – GMT +03:00. Указание часового пояса необходимо, для журналирования событий, и для точности приема сообщений о НСД [9,10, 25].

Рисунок 9 –Пример конфигурационного файла

На экране появится меню настроек криптографического шлюза FILIAL_ORG.

Необходимо перейти к закладке «Интерфейсы« и нажать кнопку «Добавить...», ввести в поля диалога информацию для IPv4, необходимую для регистрации КШ [10]:

– интерфейс Ie0 – это внешний интерфейс, его IP адрес: 200.200.2.1 с 24 маской, т.е. 255.255.255.0;

– интерфейс Ie1 – это внутренний интерфейс, его IP адрес: 192.168.2.1 с 24 маской, т.е. 255.255.255.0;

– интерфейс Ie2 – это резервный интерфейс КШ, в поле «Режим» – Автовыбор, значение MTU – 1500. (У интерфейсов со статусом «Резервирование КШ» или «SNAP-порт» не может быть установлен IP-Адрес.) Окно настройки свойств криптошлюза изображено на рисунке 10.

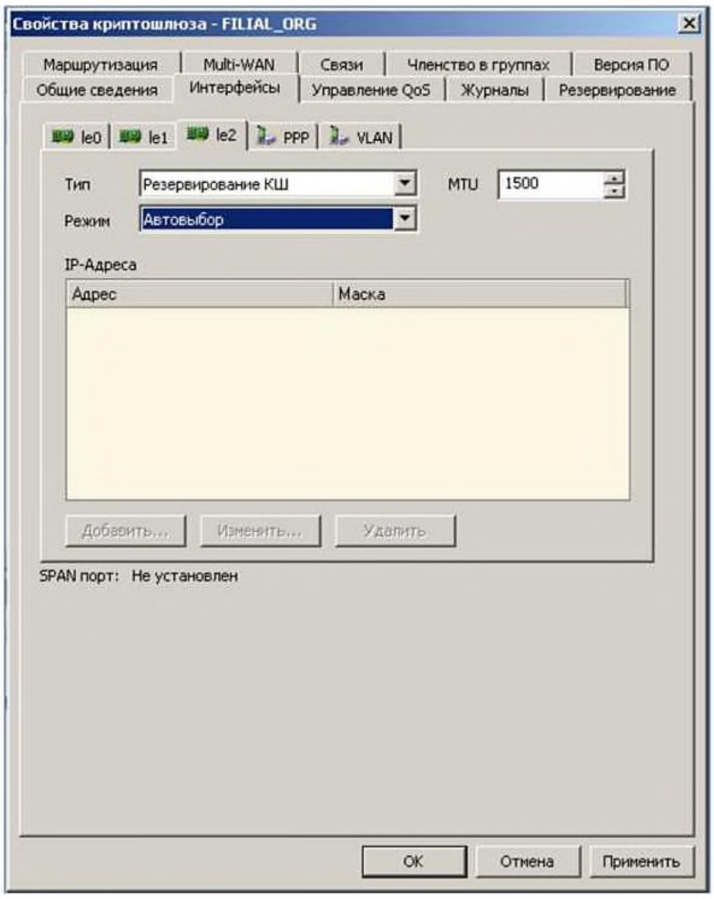

Рисунок 10 – Окно настройки свойств криптошлюза

Ввод IP-Адреса выполняется после заполнения полей «Адрес» и «Маска» и нажатия кнопки «ОК». После выполнения установки IP-Адресов интерфейсов необходимо нажать кнопку «Применить».

Далее, необходимо добавить «Маршрут по умолчанию». Для этого необходимо перейти на вкладку «Маршрутизация» выбрать «Статическая» и выполнить настройки, нажав кнопку «Добавить», а также «ОК» в окне программы [10]:

- выбрать IPv4;
- в поле «Адрес»: 0.0.0.0;
- в поле «Маска»: 0.0.0.0;
- в поле «Следующий узел»: 200.200.2.1.

Для завершения настройки следует нажать кнопку «ОК». В список КШ в основном окне Программы управления будет добавлен объект с заданным

именем, при этом его состояние будет: «Отключен (Не введен в эксплуатацию)».

Для сохранения конфигурации, необходимо подключить USB Flash.

В основном окне Программы управления в контекстном меню зарегистрированного КШ, с помощью правой кнопкой мыши войти в контекстное меню и активировать команду «Сохранить конфигурацию». И в окне «Сохранение конфигурации КШ» назначить и подтвердить пароль, с помощью которого будет ограничен доступ к сохраняемой конфигурации КШ. Длина пароля должна составлять от 5 до 14 символов. Этот пароль запрашивается при считывании конфигурации криптографическим шлюзом. При вводе пароля запрещается использовать символы кириллицы [10,19].

Далее необходимо [10,12,13]:

– указать режим работы КШ «Основной»;

– определить место сохранения конфигурации. Для этого нажать на кнопку в правой части поля, в открывшемся стандартном диалоге сохранения файла указать USB Flash и сохранить конфигурацию под именем «gate.cfg»;

– нажать кнопку "ОК". (После успешного завершения записи конфигурации КШ на экране появится сообщение об этом.);

– закрыть окно этого сообщения.

После этого необходимо сохранить текущие ключи на Flash носитель. Для этого нужно вызвать контекстное меню данного КШ и выбрать соответствующий пункт «Сохранить текущие ключи на носитель...». В появившемся окне нужно опять ввести пароль [10,13, 19].

Далее необходимо отключить Flash и ввести КШ в эксплуатацию, для этого нужно снова в окне «Свойства криптошлюза FILIAL_ORG» зайти во вкладку «Общие сведения» и поставить галочку возле пункта «Введен в эксплуатацию».

3.3.2 Настройка связи криптографических шлюзов

Для настройки связи этого КШ необходимо перейти во вкладку «Связи» и проверить, перенесен ли из левого списка в правый «КШ с ЦУСом», если нет, то перенести выделенный КШ или весь список в правую часть, нажать «ОК».

На компьютере с установленной программой управления в сети Филиал, подключить криптошлюз и загрузить операционную систему. При загрузке выбрать версию криптошлюза (IPC-100 MS-92E3), а так же ввести конфигурацию. После появления надписи «Инсталляция произошла успешно», подключить Flash носитель, с сохраненной на нем конфигурацией и в появившемся окне ввести пароль [10,11].

При удачном считывании конфигурации с USB Flash на экране появится сообщение о количестве интерфейсов и об их адресах. В последующих вопросах о предлагаемых ключах набирать «1» и «Enter».

Далее появится сообщение «Выберете пароль для:». Необходимо ввести пароль, заданный при записи ключей на носитель, и нажмите клавишу «Enter».

Для проверки работы КШ сети Филиал необходимо на компьютере с ПУ. создать правило фильтрации, разрешающее прохождение пакетов из сети «Главного офиса» в «Филиал» по протоколу ICMP (ping). (Для создания такого правила фильтрации сначала необходимо создать сетевой объект «Филиал» (IP: 192.168.2.0 255.255.255.0) с типом привязки «Защищаемый», для криптошлюза «FILIAL_ORG» и интерфейсом привязки «1e1».)

Для создания правила фильтрации необходимо вызвать список сетевых объектов, для этого в левой части окна программы управления нужно выбрать папку «Центр управления сетью \ Сетевые объекты». В правой части окна отобразится перечень сетевых объектов [10].

Вызовите меню «Операции» и активируйте команду «Создать сетевой объект» На экране появится окно настройки параметров сетевого объекта.

Далее необходимо настроить параметры сетевого объекта [10]:

- в поле «Название» – Филиал;
- поле «Описание» можно оставить пустым;
- выбрать пункт «Unicast»;

– IP: 192.168.2.0 255.255.255.0;

– Тип привязки – защищаемый;

– Криптошлюз – FILIAL_ORG;

– интерфейс - 1e1.

Для окончания, нажать на кнопку «ОК».

Выберите папку «Центр управления сетью \ Правила фильтрации». В правой части окна отобразится список правил фильтрации IP-пакетов.

Для создания правила необходимо вызвать контекстное меню в любом месте списка правил и активировать команду «Создать правило фильтрации» или нажать одноименную кнопку на панели инструментов. На экране появится диалог «Правило фильтрации» (рисунок 11) [10].

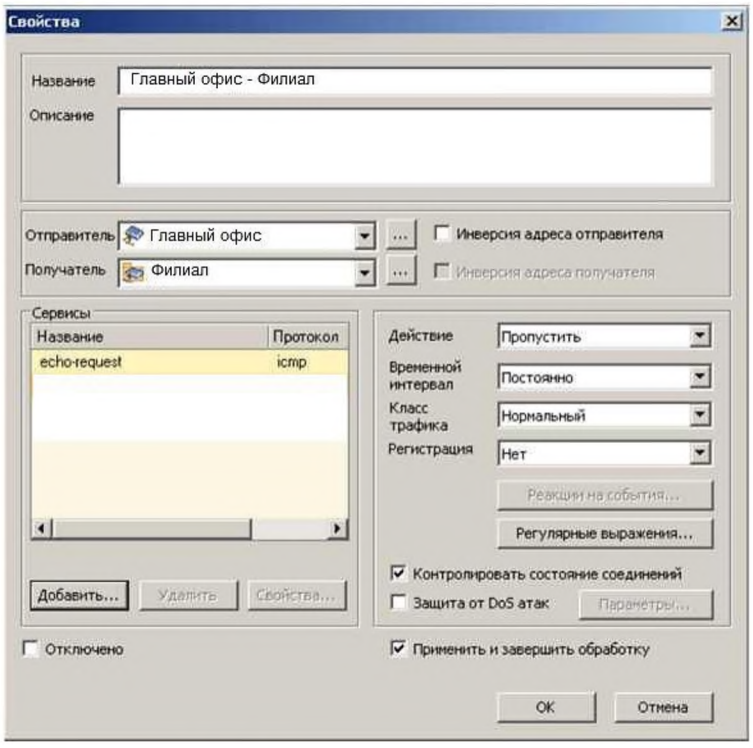

Рисунок 11 – Создание правил фильтрации

Для того чтобы это правило применилось необходимо нажать кнопку «Сохранить изменения» на панели инструментов [10].

Проверить правильность можно с АРМ с ПУ Главного офиса, выполнив в командной строке команду ping 192.168.2.2.

Перед этим необходимо проверить, работает ли опрашиваемый узел Филиала с IP адресом 192.168.2.2. Может понадобиться некоторое время для установления шифрованного канала, поэтому придется подождать результатов корректного выполнения команды [10].

3.3.3 Организация VPN типа «Шлюз - Шлюз» с другими сетями.

Собственная инфраструктура открытых ключей предназначена для установки защищенного соединения с внешней криптографической сетью. Удостоверяющим центром является ЦУС. Здесь выполняются генерация ключевой пары и издание сертификата открытого ключа, а также их хранение. Управление ключами может осуществляться по схеме одно летнего хранения и по схеме трехлетнего хранения. В рассматриваемом случае рекомендуется рассмотреть управление ключами по схеме однолетнего хранения [10, 11].

Для создания сертификата «Главного офиса», в левой части окна программы управления необходимо выбрать папку «Центр управления сетью > Сертификаты»

В правом окне программы управления, в меню Сертификаты нажать кнопку «Создать сертификат»

В окне программы «Сертификат» необходимо заполнить все свободные строки, как показано на рисунке 12, и нажать кнопку "ОК"[10, 13]:

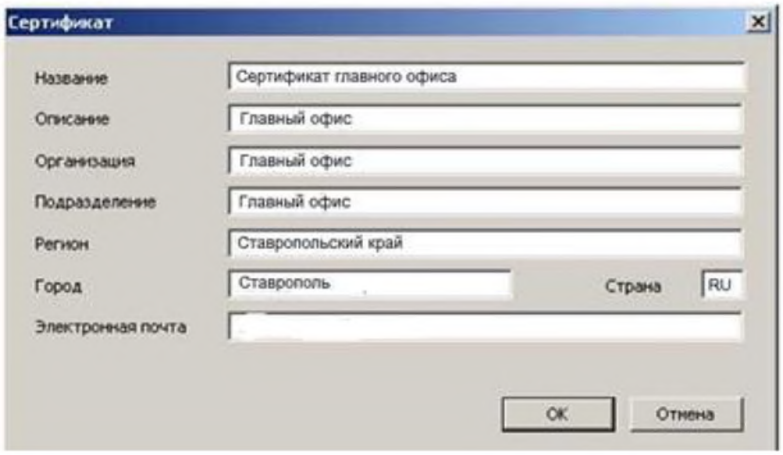

Рисунок 12 – Создание сертификата

Действие нового сертификата начинается, как правило, через 4 часа после его заведения в ПУ ЦУС. До этого момента, сертификат является не активным и подсвечивается красным.

На компьютере с ПУ филиала необходимо выполнить экспорт сертификата «Сертификат филиала» на внешний Flesh-носитель (Filial.cer), для этого нужно вызвать свойства сертификата, выбрать закладку «Details» и нажать кнопку «Copy to file...»[10, 25].

Далее данный носитель необходимо подключить (или передать защищенным способом информацию) к компьютеру с ПУ Главного офиса.

В левой части окна программы управления ПУ ЦУС необходимо выбрать папку «Внешние криптографические сети», ав правом окне программы управления, в меню управления выбрать кнопку «Создать внешнюю криптографическую сеть». В окне программы «Внешняя криптографическая сеть» заполнить все свободные строки и нажать кнопку «ОК».

В левом окне программы управления выбрать образовавшийся объект «Филиал ».Выбрать папку «Сертификаты».

В правом окне программы управления, в меню «Сертификаты» выбрать кнопку «Импортировать сертификат внешней сети» [10].

В открывшемся меню выбора файла выбрать, сохраненный ранее файл сертификата Filial.cer.

В правом окне программы управления, в меню «Сертификаты» должен отобразиться импортированный сертификат, как показано на рисунке 13:

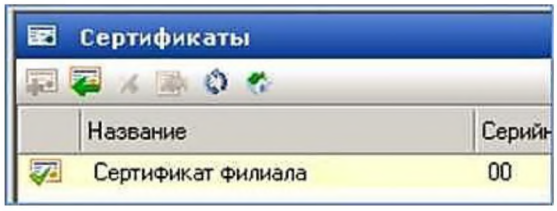

Рисунок 13 – Внешний вид меню «Сертификаты»

В левом окне программы управления необходимо выбрать объект «Филиал» и его папку «Межсетевые ключи».

В правом окне программы управления, в меню «Межсетевые ключи» выбрать кнопку «Создать межсетевой ключ».

В окне выбора сертификатов сетей выбрать сертификат своей («Главный офис») и связываемой сети («Филиал»).

Будет создан межсетевой ключ и указаны его основные параметры (срок действия, хеш-функция и др.).

В правом окне программы управления, в меню «Внешние криптографические сети» выбрать кнопку «Экспортировать конфигурацию для внешней сети».

В окне программы «Экспорт конфигурации для внешней сети» в поле «Сертификат своей сети» нажать кнопку «Выбрать...», выбрать сертификат «Главного офиса» и нажать на «ОК».

В окне программы «Экспорт конфигурации для внешней сети» в поле «Сертификат внешней сети» следует нажать кнопку «Выбрать...», и выбрать сертификат «Сертификат филиала» и нажать кнопку "ОК".

В окне программы «Экспорт конфигурации для внешней сети» в поле «Сетевые объекты и криптошлюзы, доступные для внешней сети» нажать кнопку «Добавить...».

В окне программы «Экспорт конфигурации для внешней сети» в поле «Имя файла для сохранения экспортируемой конфигурации» нажать кнопку «Выбрать...»[10].

Обязательно нужно проверить подключение Flesh-носителя к компьютеру с ПУ Главного офиса, в случае необходимости подключить его. В открывшемся окне сохранения файла выбрать Flesh-носитель и задать имя файла (например GlavniyOfis). Файл сохранится E:\GlavniyOfis.nc, далее нажать кнопку "ОК".

В ПУ ЦУС в Главном офисе необходимо выполнить экспорт сертификата. «Сертификат главного офиса» на внешний Flesh-носитель (например GlavniyOfis.cer) по аналогии с экспортом сертификата, описанным выше.

На компьютере Филиала в ПУ необходимо выполнить импорт сертификата и импорт конфигурации внешней сети (созданный файл

GlavniyOfis.nc), по аналогии с выше изложенным материалом, а так же создать межсетевой ключ [10, 26].

Там же, в меню «Внешние криптографические сети» выполнить «Экспортировать конфигурацию для внешней сети» и сохранить конфигурацию в файл Filial.nc на внешний Flesh- носитель.

Далее подключить внешний Flesh-носитель к ПУ компьютера Главного офиса и выполните импорт конфигурации «Филиал» из сохраненного файла Filial.nc.

На ПУ компьютера Главного офиса, в ПУ ЦУС необходимо зайти в свойства объектов FILIAL ORG и КШ с ЦУСом и выбрать вкладку «Связи».

Добавить в список связанных криптошлюзов объекты внешней сети «Филиал»[10].

(Это необходимо выполнить в связи с тем, что криптотоннели в АПКШ «Континент» устанавливаются только со связанными криптошлюзами.)

Для объединения сетей необходимо создать правила фильтрации:

В ПУ Главного офиса создать правило фильтрации, разрешающее прохождение ICMP трафика из сети «Филиал» (192.168.2.0/24) в сеть «Главный офис» (192.168.1.0/24).

В ПУ Филиала, также, создайте правило фильтрации, разрешающее прохождение ICMP трафика из сети «Филиал» (192.168.2.0/24) в сеть «Главный офис» (192.168.1.0/24).

Также, следует иметь в виду, что объекты сетей, которые принадлежат данной сети в ПУ ЦУС, отображаются синим цветом, а объекты внешних сетей - розовым. Объединять можно только те объекты внешних сетей, которые имеют статус «Защищаемый»[10].

Для проверки работы правил фильтрации, необходимо отправить ping ping 192.168.1.2 с узла (192.168.2.2) в филиале.

Ping прошёл успешно, значит правила работают, настройка завершена.

*Более подробные рекомендации можно найти в курсе Информ защиты АПКШ «Континент» Руководство слушателя.

3.4 Выводы по разделу

В данном разделе были разработаны общие рекомендации по защите сети, рекомендации по созданию защищенного VPN соединения при помощи криптошлюзов «Континент» версии 3.7 IPC – 100. Так же была разработана структура сети, с учетом сети филиала, и нового оборудования и адресации.

В начале раздела указаны общие сведения и рекомендации по установке оборудования и программного обеспечения, предложны схемы работы криптошлюзов в сети с маршрутизаторами. Указаны сведения о необходимом оборудовании и его назначении, а так же об особенностях операционной системы, для установки программы управления.

После общего описания, разработан подробный алгоритм настройки VPN и правил фильтрации, с дополнениями, для данной организации, в соответствии с модернизированный сетью организации. После настройки, была выполнена проверка работы VPN и правил фильтрацией отправкой ping, проверка работы сети прошла успешно.

4 Технико-экономическое обоснование предложенных рекомендаций

Экономическая эффективность информационных процессов определяется соотношением затрат на технические средства и на заработную плату работников с результатами их деятельности.

Основным эффектом от внедрения механизмов защиты информации в сети является уменьшение вероятности реализации угроз и предотвращение несанкционированного доступа к конфиденциальной информации, утрата или разглашение которой может привести к репутационным и финансовым потерям организации [9, 16].

Затраты на разработку, закупку комплектующих и монтаж оборудования сети носят единовременный характер и при расчете эффективности учитываются вместе с дополнительными капитальными затратами.

При расчете может быть принята такая модель внедрения защищенной сети – до внедрения проекта существовала возможность утраты коммерческой информации, сопоставимая с годовым приростом прибыли организации [16].

Годовой экономический эффект от внедрения проекта сети:

$$Э = Э_г - E_н * З_{общ} \quad (3)$$

где $Э_г$ - годовой прирост прибыли после внедрения проекта;

$E_н$ - нормативный коэффициент эффективности капитальных вложений (для автоматизированных систем управления и проектирования $E_н$=0.33.

$E_н$=1/$T_{нок}$, $T_{нок}$ - нормативный срок окупаемости капитальных вложений, в средства автоматики и вычислительной техники он равен 3 годам);

$З_{общ.}$ – полные единовременные затраты на проектирование и создание сети.

Основываясь на данных бухгалтерских документах, чистая прибыль ООО «ЭНЕРГО» за два прошедших года (2014 и 2015) составила 1 250 000 рублей, годовой прирост прибыли $Э_г$ составляет 723 000 рублей.

4.1 Оценка риска информационной безопасности после применения рекомендаций в организации

После применения рекомендованных предложений, вероятность использования организационных уязвимостей и вероятность использования технических уязвимостей уменьшились до 0,25, т.к. появились новые технические и организационные меры защиты. А так же, после внедрения предложенного проекта, уменьшилась вероятность реализации угрозы из всего перечня актуальных угроз Ругр=0.788975.

Поэтому риск ИБ стал ниже [18]:

$$R = 0.788975 * 0.5 * 0.5 * \frac{0.25+0.25}{2} * 100\% = 4.93 \quad (2)$$

Результат ниже максимально допустимой нормы 5%, что означает, что при соблюдении рекомендаций риск информационной безопасности, незначителен, реализация угрозы несанкционированного доступа по каналам связи невозможна. Величина риска ИБ, в этом случае, в основном зависит от других угроз и показателей защищенности.

4.2 Оценка стоимости внедрения проекта

Общие затраты на проектирование и создание сети определяются по формуле (3):

$$З_{общ} = К_1 + К_2, \quad (3)$$

где $К_1$ – производственные затраты;

$К_2$ – капитальные вложения.

Оценка производственных затрат производится по формуле (4):

$$K_1 = C_1 + C_2 + C_3, \quad (4)$$

где C_1 – затраты на НИР и ТЗ;

C_2 – затраты на опытную эксплуатацию и внедрение;

C_3 – затраты на рабочий проект.

Смета производственных затрат приведена в таблице 3.

Таблица 3 – Смета производственных затрат

Производственные затраты	Сумма, руб.
Затраты на НИР и ТЗ	2000
Затраты на опытную эксплуатацию и внедрение	5000
Затраты на рабочий проект	2000
ИТОГО	9000

То есть производственные затраты составляют 9000 рублей.

Смета затрат на капитальные вложения складывается из объема инвестиций на покупку оборудования и затрат на командировочные расходы приведённых в таблице 4 и в таблице 5 [5,11,22].

Таблица 4 – Расчет объема инвестиций на покупку оборудования

Наименование	Кол-во	Стоимость	
		Удельная (руб.)	Общая (руб.)
АПКШ «Континент» 3.7. Криптошлюз. Платформа IPC-100. Inc. TS Basic lvl	1 шт	197 340 р.	197 340 р.
АПКШ «Континент» 3.7. ЦУС - Сервер Доступа. Платформа IPC-100. Inc. TS Basic lvl	1 шт	254 150 р.	254 150 р.
Ключ активации сервиса расширенной гарантии на аппаратную платформу Континент IPC-100, с заменой в течении 2-х рабочих дней, сроком на 1 год.	1 шт	30 586 р.	30 586 р.
Право на использование Континент АП (1 дополнительное подключение пользователя Континент АП к СД). Inc. TS Basic lvl	1 шт	5 800 р.	5 800 р
Установочный комплект. СКЗИ «Континент-АП» версия 3.7	2 шт	225 р.	550 р.
Ключ активации сервиса прямой технической	1 шт	91 458 р	91 458 р

Наименование	Кол-во	Стоимость	
		Удельная (руб.)	Общая (руб.)
поддержки уровня "Стандартный" для АПКШ «Континент»			
МДЗ «Соболь»	2 шт	10 350 р	20 700 р
Комплектующие			10 000 р.
Итого			610 584 р

Таблица 5 – Затраты на командировочные расходы и повышение квалификации сотрудника организации

Наименование	Ед. измерения	Кол-во	Стоимость с НДС	
			Удельная руб.	Общая в руб.
Стоимость дистанционного обучения сотрудника организации настройке оборудования «Континент»	Руб.	1	25 000	25 000
Проезд	шт.	2	240	480
Проживание	суток	3	500	1 500
Командировочные	дн.	3	200	600
ИТОГО:				27 580 ₽

Так как в филиалах организации отсутствуют специалисты должного уровня для настройки VPN на криптошлюзах «Континент», то в расходы стоит включить стоимость обучения специалиста сетевой безопасности и его командировки.

Таким образом общие затраты на проект защищенной распределенной сети с использованием технологии VPN реализованной с помощью АПКШ «Континент» составляют 638 164 рублей. (Сравнительный анализ характеристик и цен на оборудование представлен в Приложении Г).

Общие затраты на проектирование и создание сети составляют:

$$З_{общ} = К_1 + К_2 = 9000 + 638\ 164 = 647\ 164 \text{ руб.} \quad (5)$$

4.3 Расчет срока окупаемости сети и основные технико-экономические показатели

Теперь можно оценить срок окупаемости проекта:

$$Т_{ок} = З_{общ} / Э_{г} = 647\ 164 / 723\ 000 = \sim 0{,}9 \text{ года} \quad (6)$$

Таким образом, внедрение рекомендованной распределенной сети в ООО «ЭНЕРГО» помимо более эффективного решения стоящих перед организацией задач, позволяет устранить вероятные риски, связанные с утратой конфиденциальной информации организации. Среднее время окупаемости затрат на внедрение спроектированной сети составляет 9 месяцев.

4.4 Выводы по разделу

В данном разделе был рассчитан риск ИБ после внедрения сети с предложенными рекомендациями в организацию. Риск уменьшился, за счет уменьшения количества вероятных угроз, и стал менее 5%, т.е. в пределах нормы, что доказывает эффективность введенных мер защиты от несанкционированного доступа через распределенную сеть.

В качестве технико-экономического обоснования приведены таблицы с приведенными объемами инвестиций на покупку оборудования и командировочные специалиста по сетевой безопасности.

Были рассчитаны затраты на рекомендованный проект сети, затраты составили 647 164 рублей, при помощи формулы (6) выяснено, что проект сети окупиться примерно через девять месяцев после его установки, без учета ежемесячного ущерба, до установки рекомендованной сети. Ущерб до внедрения предложенной сети примерно, в среднем, был бы равен объему ежемесячной прибыли, или вполовину больше этой суммы, т.е. около 100 тысяч рублей, после внедрения – от 1 000 до 10 000 рублей, с учетом оставшихся возможных угроз.

Заключение

В данной выпускной квалификационной работе выполнен анализ распределенной сети организации ООО «ЭНЕРГО» с целью выявления угроз, которым она может быть подвержена. Выяснено, что наибольший коэффициент реализуемости угрозы присвоен угрозам несанкционированного доступа через распределенную сеть организации, а так же выяснено, что риск ИБ превышает максимально допустимое значение. В результате анализа выявлены основные угрозы, требующие реализации проекта, удовлетворяющего следующим требованиям:

– обеспечение защиты информационного трафика во время прохождения открытых участков сети за пределами контролируемой зоны;

– обеспечение полной невидимости виртуальной защищенной сети для пользователей не входящих в данную сеть;

– обеспечение защиты от несанкционированного доступа к узлам сети головного офиса и филиалов.

По итогам первого раздела было выявлено, что наиболее приемлемым вариантом для построения защищенного канала между главным офисом и филиалом является виртуальная частная сеть. Перед реализацией разработанных рекомендаций по построению распределенной сети был проведен сравнительный анализ методов и средств развертывания VPN каналов между главным офисом и филиалом. Приведены признаки для классификации технологии VPN. В результате сравнительного анализа решено использовать метод реализации виртуальной частной сети типа сеть-сеть на базе программно-аппаратных средств. По итогам сравнительного анализа, выбран наиболее подходящий вариант – АПКШ «Континент». Его отличительной чертой является то, что он имеет все необходимые сертификаты ФСБ и ФСТЭК, и он представляет собой цельный аппаратно-программный продукт.

В качестве проекта защищенной распределенной сети приведены структурные схемы сети организации с изображением оборудования, установленного в главном офисе и филиале и топологии сети. Так же

приведены подробные инструкции, по настройке сетевого оборудования, и настройки VPN.

В результате реализации проекта защищенной распределенной сети с использованием АПКШ «Континент» в организации удовлетворены все требования, сформированные в ходе анализа сети. Технико-экономическое обоснование полностью оправдывает реализацию данного проекта в ООО «ЭНЕРГО».

Задачи, поставленные для достижения цели, выполнены:

– проанализирована комплексная система защиты информации организации;

– проведен сравнительный анализ существующих методов и средств реализации VPN при построении защищенных распределенных сетей;

– разработаны рекомендации по построению защищенной распределенной сети организации с использованием АПКШ «Континент»;

– составлено технико-экономическое обоснование.

Разработанные мероприятия обеспечивают повышение уровня информационной безопасности в организации, и снижают риск информационной безопасности.

Теоретическая значимость работы состоит в том, то в ней собран достаточно большой объем информации по заданной в выпускной квалификационной работе теме и эта информация систематизирована, раскрыт и уточнен понятийный аппарат проблемы. Тема ВКР прошла апробацию в научных конференциях. (Приложение Д)

Практическая ценность работы заключается в том, что разработанные рекомендации можно в дальнейшем применять для решения проблем, связанных с формированием распределенной сети организации и защитой данных передаваемых по этой сети.

В дальнейшем весь материал дипломной работы можно применять не только для дальнейшего исследования, так же разработанный проект сети может быть использован в качестве типового проекта для создания схожих по структуре распределенных сетей небольших организаций.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Галатенко В.А. Стандарты информационной безопасности: Курс лекций. – М.: ИНТУИТ, 2013. – 253 с.;

2 ГОСТ 28147-89 Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – Введ.01.01.1990. – М.: Изд.стандартов, 2002.;

3 Браун С. Виртуальные частные сети VPN. – СПб.: Питер, 2014. – 435с.;

4 Волчихин В. И., Механов В. Б., Вашкевич Н. П., Макарычев П. П. Новые информационные технологии и системы : сб. науч. ст. XI Междунар. науч.-техн. конф.– Пенза :Изд-во ПГУ, 2014. – 444 с.

5 Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 ФСТЭК России [Электронный ресурс], – http://fstec.ru/ – сайт в интернете (дата обращения 12.04.2016)

6 Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. - М.: Издательство Логос; ПБОЮЛ, 2001. – 264 с;

7 Запечников С. В., Милославская Н. Г., Толстой А. И., Ушаков Д. В. Информационная безопасность открытых систем. – Том 1, Угрозы, уязвимости, атаки и подходы к защите – М: Горячая линия – Телеком, 2013 – 532 с.;

8 Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях. – М.: КУДИЦ-ОБРАЗ, 2015. – 368 с.;

9 Исамидинов А. Н. Защита коммерческой тайны в сфере трудовых отношений. №11. М.: Издательство Книжный дом «ЛИБРОКОМ», 2014. – 120с.

10Код безопасности. Континент. [Электронный ресурс], – http://www.securitycode.ru/ – статья в интернете.

11 Код безопасности. АПКШ «Континент». Расчет стоимости. [Электронный ресурс], – http://www.securitycode.ru/where_to_buy/calc/kontinent/ – статья в интернете (дата обращения 05.05.2016)

12 Колесников О.В, Хетч Б., LINUX. Создание виртуальных частных сетей (VPN) – Москва: Издательство "КУДИЦ-ОБРАЗ",2005. – 454 с.

13 Кульгин М.В. Технологии корпоративных сетей. Энциклопедия. – СПб.: Питер, 2013. – 704 с.;

14 Локхарт Э. Антихакинг в сети. Трюки. журнал Изд-во- СПб.: Питер, 2005. – 296 с: ил.;

15 Мельников В.П. Информационная безопасность и защита информации: учеб.пособие для студ. учреждений высш. проф. образования. – М. : Издательский центр «Академия», 2012. – 336с.;

16 Мельников В. В., Защита информации в компьютерных системах. – М.: Финансы и статистика, – 2011– 45 с.;

17 Олифер В. Г., Олифер Н. А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. – СПб.: Питер, 2014. – 672 с.;

18 Плетнев П. В., Белов В. М. Методика оценки рисков информационной безопасности на предприятиях малого и среднего бизнеса // Доклады Томского государственного университета систем управления и радиоэлектроники – Томск: Изд-во ТУСУР, 2012. – С.83–86.;

19 Романец Ю. В.. Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. 2-е изд. – М: Радио и связь, 2013. –328 с.;

20 Рябко Б. Я., Фионов А. Н. Криптографические методы защиты информации. – 2-е изд. – М.: Горячая линия – Телеком, 2013. – 229 с.;

21 Сериков И.В Введение в Виртуальные Частные Сети (VPN) [Электронный ресурс], – http://www.hub.ru/archives/2269/ – статья в интернете.

22 Ульянинкова О.В. Российский рынок сертифицированных средств защиты информации для ОС GNU/Linux [Электронный ресурс], – http://www.pcweek.ru/security/article/detail.php?ID=167145 – статья в интернете.

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

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

25 Фролов А. В., Фролов Г. В. Глобальные сети компьютеров.– М.: Диалог-МИФИ, 1996. – 228 с;

26 Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие. – М.: ИД «ФОРУМ»: ИНФРА-М, 2011. – 416 с.

ПРИЛОЖЕНИЕ А

(обязательное)

Перечень конфиденциальных сведений

Таблица А.1 – Перечень сведений являющихся ценными для организации

№ № п/п	Наименование сведений	Гриф конф-ти	Срок конф-ти
Данные об организации			
1	Персональные данные клиентов организации	Для служебного пользования (Д.с.п)	До прекращения существования организации (постоянно)
2	Персональные данные сотрудников организации	Д.с.п.	Постоянно
3	Персональные данные контрагентов	Д.с.п.	Постоянно
4	Учредительные документы (устав, свидетельство и др.)	Д.с.п.	До изменения
5	Перечень структурных подразделений, филиалов, участков с указанием данных о структуре взаимодействия с главном офисом	Д.с.п.	До изменения
6	Сведения о производстве и управлении	Д.с.п	Постоянно
7	Наличие судебных исков	Д.с.п	5 лет
8	Фактические сведения о численности и фонде заработной платы работников организации	Д.с.п.	1 год
9	Протоколы совещаний	Д.с.п	2-3 года
10	Сведения о переговорах	Д.с.п	3 года
11	Сведения о кадровом составе, штатном расписании	Д.с.п.	1 год
12	Отчеты аудиторов	Д.с.п	3-5 лет
13	Копии лицензий на осуществление профессиональной деятельности	Д.с.п.	До окончания срока лицензии
14	Договора аренды, лизинга, залога	Д.с.п	До расторжения
15	Копии правоустанавливающих документов на земельные участки	Д.с.п.	Постоянно
Научная деятельность			
16	Материалы об открытиях и изобретениях, сделанных в организации и имеющих крупное научное значение	Д.с.п.	5 лет
17	Сведения о сотрудниках, сделавших открытие, и о тех. средствах на которых оно применено	Д.с.п.	3 года
18	Бухгалтерская отчетность, первичная документация	Д.с.п.	1 год

№ № п/п	Наименование сведений	Гриф конф-ти	Срок конф-ти
19	Сведения об уплаченных налогах и сборах	Д.с.п.	Постоянно
20	Полные плановые или отчетные данные о вводе в действие основных фондов, об объемах капитальных вложений или строительно-монтажных работ	Д.с.п.	3 года
21	Плановые экономические показатели	Д.с.п.	1 год
22	Сведения о модернизации ранее известных технологий, процессов и оборудования, позволяющих повысить конкурентоспособность	Д.с.п.	5 лет
Валютно-финансовые вопросы			
23	Плановые и фактические показатели финансового плана организации	Д.с.п.	До реализации
24	Показатели рентабельности	Д.с.п	2 года
25	Сведения, раскрывающие директивы по проведению переговоров, в т.ч. границы полномочий должностных лиц по ценам, скидкам и другим условиям	Д.с.п.	5 лет
26	Результаты финансово-хозяйственной деятельности организации за квартал или год	Д.с.п.	1 год
27	Сведения об основных заказчиках услуг	Д. с.п.	Постоянно
Планы			
28	Сведения о дальнейших планах сотрудничества с другими организациями (разрыве соглашений)	Д.с.п.	До реализации
29	Прогноз капиталовложений на пять лет	Д.с.п.	До реализации и после 5 лет
30	Прогноз ближайших изменений в деятельности организации и в отрасли	Д.с.п.	1 год
31	Управленческие решения, планы развития производства, инвестиционные программы	Д.с.п.	3 года
32	Сведения о покупке, размещении и настройке нового оборудования	Д.с.п.	3 года
Система безопасности организации			
33	Сведения, раскрывающие систему, средства защиты информации ЛВС организации от НСД, а также значения действующих кодов и паролей	Д.с.п.	Постоянно
34	Должностная инструкция сотрудника отдела защиты информации	Д.с.п.	До внесения изменений
35	Требования по обеспечению сохранения служебной тайны при выполнении работ в организации.	Д.с.п.	3 года
36	Порядок передачи служебной информации ограниченного распространения другим организациям	Д.с.п.	5 лет

№ № п/п	Наименование сведений	Гриф конф-ти	Срок конф-ти
37	Сведения о состоянии программного и компьютерного обеспечения	Д.с.п.	Постоянно
38	Сведения об используемых методах защиты информации в организации	Д.с.п.	Постоянно
39	Сведения о размещении систем видеонаблюдения, технических средствах защиты информации, кпп, и тд.	Д.с.п.	До изменения
40	Сведения о размещении и сохранении ключей, идентификаторов.	Д.с.п.	2 года
41	Сведения о степени защищенности помещений для переговоров, серверных, так же помещений для обработки ПДн	Д.с.п.	3 года
42	Сведения о месте и порядке уничтожения устаревших данных (ПДн)	Д.с.п.	4 года

ПРИЛОЖЕНИЕ Б

(обязательное)

Модель угроз

1. Частная модель угроз безопасности персональных данных при их обработке в информационной системе ООО «ЭНЕРГО» и при передачи

ПОКАЗАТЕЛИ ИСХОДНОГО УРОВНЯ ЗАЩИЩЕННОСТИ ИСПДн

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1).

В таблице Б.1 представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица Б.1 – Характеристики уровня исходной защищенности

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению: Локальная ИСПДн, развернутая в пределах одного здания	+	–	–
2. По наличию соединения с сетями общего пользования: ИСПДн, физически отделенная от сети общего пользования	–	–	+
3. По встроенным (легальным) операциям с записями баз персональных данных: чтение, поиск, запись, удаление, сортировка	–	+	–
копирование, модификация, передача	–	+	–
4. По разграничению доступа к персональным данным: ИСПДн, к которой имеют доступ определенные перечнем сотрудники Общества	–	+	–
6. По уровню обобщения (обезличивания) ПДн: ИСПДн, в которой данные обезличиваются только при передаче в другие организации и не обезличены при предоставлении пользователю в организации	–	+	–
7. По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: предоставляющая часть ПДн	+	–	–

ВЫВОД: ИСПДн имеет средний уровень исходной защищенности, так как более 70% характеристик соответствуют уровню не ниже «средний». Показатель исходной защищенности Y_1=5*.

* - Исходная степень защищенности определяется следующим образом:

ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу) (Y_1= 0).

ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные - низкому уровню защищенности (Y_1= 5).

ИСПДн имеет низкую степень исходной защищенности, если не выполняется условия по пунктам 1 и 2 (Y_1= 10).

ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УГРОЗ БЕЗОПАСНОСТИ ПДН

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

В таблице Б.2 приведено описание каждой угрозы и даны обобщенные вероятности реализации угроз и оценка опасности каждой угрозы для ИСПДн.

Таблица Б.2 – Вероятность реализации угроз

Тип угроз безопасности ПДн	Коэффициент вероятности реализации (Y2)*	Вероятность реализации угрозы
1. Угрозы от утечки по техническим каналам		
1.1. Угрозы утечки акустической информации	5	средняя
1.2. Угрозы утечки видовой информации	2	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	0	маловероятная
2. Угрозы несанкционированного доступа к информации		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0	маловероятная
2.1.2. Кража носителей информации	0	маловероятная
2.1.3. Кража ключей и атрибутов доступа	2	низкая
2.1.4. Кражи, модификации, уничтожения информации	0	маловероятная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0	маловероятная

Тип угроз безопасности ПДн	Коэффициент вероятности реализации (Y2)*	Вероятность реализации угрозы
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0	маловероятная
2.1.7. Несанкционированное отключение средств защиты	0	маловероятная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
2.2.1. Действия вредоносных программ (вирусов)	5	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0	маловероятная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	0	маловероятная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т.п.) характера		
2.3.1. Утрата ключей и атрибутов доступа	5	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0	маловероятная
2.3.3. Непреднамеренное отключение средств защиты	0	маловероятная
2.3.4. Выход из строя аппаратно-программных средств	0	маловероятная
2.3.5. Сбой системы электроснабжения	0	маловероятная
2.3.6. Стихийное бедствие	2	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами, не допущенными к ее обработке	0	маловероятная
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	2	низкая
2.5.Угрозы несанкционированного доступа по каналам связи		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	10	высокая
2.5.1.1. Перехват за переделами с контролируемой зоны	5	средняя
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0	маловероятная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0	маловероятная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	2	низкая

Тип угроз безопасности ПДн	Коэффициент вероятности реализации (Y2)*	Вероятность реализации угрозы
2.5.3.Угрозы выявления паролей по сети	5	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	10	средняя
2.5.5.Угрозы подмены доверенного объекта в сети	10	средняя
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	10	средняя
2.5.7.Угрозы типа «Отказ в обслуживании»	2	низкая
2.5.8.Угрозы удаленного запуска приложений	2	низкая
2.5.9.Угрозы внедрения по сети вредоносных программ	2	низкая

* - Числовой коэффициент (Y_2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

– маловероятно - отсутствуют объективные предпосылки для осуществления угрозы ($Y_2 = 0$);

– низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию ($Y_2 = 2$);

– средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны ($Y_2 = 5$);

– высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты ($Y_2 = 10$).

ОЦЕНКА ВОЗМОЖНОСТИ РЕАЛИЗАЦИИ УГРОЗ

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$.*

В таблице Б.3 приведено описание угрозы, дан расчетный коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы.

Таблица Б.3 – Коэффициент реализуемости угрозы

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам		
1.1. Угрозы утечки акустической информации	0,5	средняя
1.2. Угрозы утечки видовой информации	0,35	средняя

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,35	средняя
2.1.4. Кражи, модификации, уничтожения информации	0,25	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
2.1.7. Несанкционированное отключение средств защиты	0,25	низкая
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)		
2.2.1. Действия вредоносных программ (вирусов)	0,5	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	0,25	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т.п.) характера		
2.3.1. Утрата ключей и атрибутов доступа	0,5	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,25	низкая
2.3.3. Непреднамеренное отключение средств защиты	0,25	низкая
2.3.4. Выход из строя аппаратно-программных средств	0,25	низкая
2.3.5. Сбой системы электроснабжения	0,25	низкая
2.3.6. Стихийное бедствие	0,35	средняя
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами не допущенными к ее обработке	0,25	низкая
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,35	средняя

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
2.5.Угрозы несанкционированного доступа по каналам связи		
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	0,75	высокая
2.5.1.1. Перехват за переделами с контролируемой зоны	0,5	средняя
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,35	средняя
2.5.3.Угрозы выявления паролей по сети	0,5	средняя
2.5.4.Угрозы навязывание ложного маршрута сети	0,75	высокая
2.5.5.Угрозы подмены доверенного объекта в сети	0,75	высокая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,75	высокая
2.5.7.Угрозы типа «Отказ в обслуживании»	0,35	средняя
2.5.8.Угрозы удаленного запуска приложений	0,35	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	0,35	средняя

* - Рассчитанный по формуле $Y=(Y_1+Y_2)/20$ коэффициент реализуемости угрозы определяется по следующим диапазонам: $0>Y>0,3$ – низкая; $0,3>Y>0,6$ – средняя; $0,6>Y>0,8$ – высокая; $Y>0,8$ – очень высокая.

ОЦЕНКА ОПАСНОСТИ КАЖДОЙ УГРОЗЫ

Оценка опасности угрозы определяется на основе опроса специалистов по вербальным показателям опасности с тремя значениями:

– низкая опасность – если реализация угрозы может привести к незначительным негативным последствиям для субъектов персональных данных;

– средняя опасность – если реализация угрозы может привести к негативным последствиям для субъектов персональных данных;

– высокая опасность – если реализация угрозы может привести к значительным негативным последствиям для субъектов персональных данных.

Таблица Б.4 – Оценка опасности угрозы

Тип угроз безопасности ПДн	Опасность угрозы
1. Угрозы от утечки по техническим каналам	
1.1. Угрозы утечки акустической информации	низкая
1.2. Угрозы утечки видовой информации	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	средняя
2. Угрозы несанкционированного доступа к информации	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	низкая
2.1.2. Кража носителей информации	средняя
2.1.3. Кража ключей и атрибутов доступа	низкая
2.1.4. Кражи, модификации, уничтожения информации	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	средняя
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	средняя
2.1.7. Несанкционированное отключение средств защиты	средняя
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
2.2.1. Действия вредоносных программ (вирусов)	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	средняя
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	низкая
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т.п.) характера	
2.3.1. Утрата ключей и атрибутов доступа	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	средняя
2.3.4. Выход из строя аппаратно-программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	средняя
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами не допущенными к ее обработке	средняя

Тип угроз безопасности ПДн	Опасность угрозы
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	средняя
2.5.Угрозы несанкционированного доступа по каналам связи	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	высокая
2.5.1.1. Перехват за переделами с контролируемой зоны	высокая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	средняя
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	средняя
2.5.3.Угрозы выявления паролей по сети	высокая
2.5.4.Угрозы навязывание ложного маршрута сети	высокая
2.5.5.Угрозы подмены доверенного объекта в сети	высокая
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	средняя
2.5.7.Угрозы типа «Отказ в обслуживании»	средняя
2.5.8.Угрозы удаленного запуска приложений	средняя
2.5.9.Угрозы внедрения по сети вредоносных программ	средняя

ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ В ИСПДн

Классификация угроз на актуальные и неактуальные производится по правилам, разработанным в Методике определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, которая утверждена ФСТЭК России 14.02.2008 года. Определение угроз осуществляется на основе ниже приведенной таблицы Б.5:

Таблица Б.5 – Определение актуальности угроз

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

Обобщенный список актуальных угроз в ИСПДн представлен в таблице Б.6.

Таблица Б.6 – Обобщенный список актуальных угроз

Тип угроз безопасности ПДн	Актуальность угрозы
1. Угрозы от утечки по техническим каналам	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
2.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)	
2.2.1. Действия вредоносных программ (вирусов)	актуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	неактуальная
2.3. Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и систем защиты ПДн в ее составе из-за сбоев в программном обеспечении, а также от сбоев аппаратуры, из-за ненадежности элементов, сбоев электропитания и стихийного (ударов молний, пожаров, наводнений и т.п.) характера	
2.3.1. Утрата ключей и атрибутов доступа	актуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	неактуальная
2.3.3. Непреднамеренное отключение средств защиты	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	актуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	

Тип угроз безопасности ПДн	Актуальность угрозы
2.4.1. Доступ к информации, копирование, модификация, уничтожение, лицами не допущенными к ее обработке	неактуальная
2.4.2. Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	актуальная
2.5.Угрозы несанкционированного доступа по каналам связи	
2.5.1.Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	актуальная
2.5.1.1. Перехват за переделами с контролируемой зоны	актуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3.Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2.Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов, топологии сети, открытых портов и служб, открытых соединений и др.	актуальная
2.5.3.Угрозы выявления паролей по сети	актуальная
2.5.4.Угрозы навязывание ложного маршрута сети	актуальная
2.5.5.Угрозы подмены доверенного объекта в сети	актуальная
2.5.6.Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	актуальная
2.5.7.Угрозы типа «Отказ в обслуживании»	актуальная
2.5.8.Угрозы удаленного запуска приложений	актуальная
2.5.9.Угрозы внедрения по сети вредоносных программ	актуальная

ВЫВОД:

Актуальными угрозами информационной безопасности являются:

– действия вредоносных программ (вирусов);

– утрата ключей и атрибутов доступа;

– стихийное бедствие;

– разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке;

– угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;

– перехват за переделами с контролируемой зоны;

– угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых

портов и служб, открытых соединений и др.;

- угрозы выявления паролей по сети;
- угрозы навязывание ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

РЕКОМЕНДАЦИИ:

Для предотвращения реализации выявленных для ИСПД актуальных угроз, в системе защиты информационной системы должны использоваться следующие организационные, технические и программные средства:

- средства антивирусной защиты;
- средства от вторжения вредоносных модулей и программ;
- программный комплекс «Межсетевой экран»;
- средства управления доступом в систему;
- реализация парольной политики, устанавливающая обязательную сложность и периодичность смены пароля;
- методы и средства аутентификации пользователей на основе usb-ключей, паролей и логинов доступа;
- мероприятия по контролю доступа в контролируемую зону лиц, не имеющих доступа к обработке ПДн.

4 Оценка риска ИБ ИС ООО «ЭНЕРГО»

ОПРЕДЕЛЕНИЕ СТЕПЕНИ СООТВЕТСТВИИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ОРГАНИЗАЦИИ ТРЕБОВАНИЯМ НОРМАТИВНЫХ ДОКУМЕНТОВ

Любая организация, имеющая информационные системы или работа которой связана с использованием информационных технологий для ведения бизнеса, должна соблюдать федеральные законы в этой отрасли. Невыполнение данных требований может повлечь за собой гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством РФ ответственность. Алгоритм определения риска несоответствия требований законодательства в области ИБ включает в себя проведение всестороннего анализа состояния системы защиты конфиденциальной документированной информации с целью выявления выполнения требований в соответствии с требованиями

законодательства. В ходе проведения анализа всем требованиям, которые выполняются, присваивается значение «1», в противном случае – «0».

Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются.

Таблица Б.7 – Определение степени соответствии системы защиты информации организации требованиям нормативных документов

№ п/п	Нормативные документы по ИБ	Соответствие
1	Федеральный закон от 27 июля 2006 г. N 152-ФЗ "О персональных данных"	1
2	Федеральный закон от 27 июля 2006 г. N 149-ФЗ " Об информации, информационных технологиях и о защите информации"	0
3	Федеральный закон от 29.07.2004 N 98-ФЗ (ред. от 12.03.2014) "О коммерческой тайне"	0
4	Постановление Правительства РФ от 15 сентября 2008 г. N 687 "Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации"	1
5	Постановление Правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»	0
6	Постановление Правительства Российской Федерации от 21 марта 2012 г. N 211 "Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами"	1
7	Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службой по техническому и экспортному контролю 14 февраля 2008 г.)	0
8	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. Федеральной службой по техническому и экспортному контролю 15 февраля 2008 г.)	0
9	Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»	0
10	Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. N 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»	1
11	«Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», Приказ ФСТЭК России от 18 февраля 2013г. № 21.	0
12	Приказ ФСБ РФ от 09.02.2005 № 66 "Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)	0
13	«Методические рекомендации управлениям ФСТЭК России по федеральным округам об организации работ по аттестации объектов информатизации по требованиям безопасности информации», утверждены заместителем директора ФСТЭК России 25 апреля 2006г.	0

№ п/п	Нормативные документы по ИБ	Соответствие
14	«Сборник руководящих документов по защите информации от НСД», утверждены приказом председателя Государственной технической комиссии при Президенте Российской Федерации, 1998г.	0
15	«Методические документы по обеспечению ПДн при их обработке в ИСПДн», утверждены Заместителем директора ФСТЭК России 14 февраля 2008г. и 15 февраля 2008г. и Приказом ФСТЭК России от 05 февраля 2010г. № 58.	0
16	«Руководящий документ. Защита от несанкционированного доступа к информации. Термины и определения», утвержден решением председателя Гостехкомиссии России от 30 марта 1992 г.	1
17	«Общие требования по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 18 мая 2007г	0
18	«Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры», утверждены заместителем директора ФСТЭК России 19 ноября 2007г.	0
19	«Об утверждении Методических рекомендаций по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации», утверждены Приказом ФСБ Российской Федерации 21 февраля 2008г. № 149/54-144.	0
20	«Положение по аттестации объектов информатизации по требованиям безопасности информации», утверждено председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.	1
21	«Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», ФСТЭК России, 2008г., пометка «для служебного пользования» снята Решением ФСТЭК России от 16 ноября 2009г.	0

В заключение анализа необходимо определить уровень риска несоответствия требований законодательства по ИБ, который определяется по таблице Б.8.

Таблица Б.8 – Результаты анализа риска несоответствия требования законодательства в области защиты конфиденциальной информации

Сумма выполненных требований	Риск несоответствия требованиям законодательства (*Rn*)
20–31	0,01
7–19	0,25
Менее 6	0,5
Не выполняются	0,9

Таким образом, значение риска несоответствия требования законодательства в области защиты конфиденциальной документированной информации для ООО «ЭНЕРГО» равно 0,5, т.е. Rn = 0,5.

РАЗРАБОТКА МОДЕЛИ УГРОЗ ДЛЯ ЗАЩИЩАЕМОЙ ИНФОРМАЦИИ ОРГАНИЗАЦИИ

На данном этапе определяются источники угроз для выбранного типа объекта среды. Для решения задачи оценки ИБ выбираются актуальные угрозы и соответствующие типы объектов среды. В таблице Б.9 представлены типы объектов среды и актуальные угрозы для защищаемой информации.

Таблица Б.9 – Перечень актуальных угроз для информации ООО «ЭНЕРГО»

Тип угроз безопасности ПДн	Актуальность угрозы
Действия вредоносных программ (вирусов)	актуальная
Утрата ключей и атрибутов доступа	актуальная
Стихийное бедствие	актуальная
Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	актуальная
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	актуальная
Перехват за переделами с контролируемой зоны	актуальная
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	актуальная
Угрозы выявления паролей по сети	актуальная
Угрозы навязывание ложного маршрута сети	актуальная
Угрозы подмены доверенного объекта в сети	актуальная
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	актуальная
Угрозы типа «Отказ в обслуживании»	актуальная
Угрозы удаленного запуска приложений	актуальная
Угрозы внедрения по сети вредоносных программ	актуальная

ОПРЕДЕЛЕНИЕ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ УГРОЗ

В связи с тем, что на один актив могут воздействовать одновременно несколько угроз, необходимо определить вероятность того, что хотя бы одна угроза реализуется по отношению к выбранному активу.

Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз $y1$, $y2$, ..., yn, где n – количество угроз, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

В таблице 6 представлены результаты анализа вероятности реализации наиболее

актуальных угроз для конфиденциальной документированной информации в ООО «ЭНЕРГО».

Таблица Б.10 – Вероятности реализации наиболее актуальных угроз для конфиденциальной документированной информации в ООО «ЭНЕРГО».

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)
Действия вредоносных программ (вирусов)	0,5
Утрата ключей и атрибутов доступа	0,5
Стихийное бедствие	0,35
Разглашение информации, копирование, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,35
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	0,75
Перехват за переделами с контролируемой зоны	0,5
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,35
Угрозы выявления паролей по сети	0,5
Угрозы навязывание ложного маршрута сети	0,75
Угрозы подмены доверенного объекта в сети	0,75
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,75
Угрозы типа «Отказ в обслуживании»	0,35
Угрозы удаленного запуска приложений	0,35
Угрозы внедрения по сети вредоносных программ	0,35

Определение вероятности наступления неблагоприятных событий в связи с реализацией хотя бы одной угрозы из перечня актуальных угроз на рассматриваемый актив. Вероятность реализации хотя бы одной угрозы из совокупности вероятностей угроз Р*у*1, Р*у*2, ..., Р*уn*, равна разности между единицей и произведением вероятностей противоположных событий. Вероятность противоположных событий определяется как разность между единицей и вероятностью угроз.

$$Ругр = 1 - П(1 - Ру1)(1 - Ру2)(1 - Ру3) \dots (1 - Руn), \quad (Б.1)$$

где n-количество угроз

В результате проведённых расчётов вероятность реализации угроз по основным типам объектов среды:

$$P_{угр} = 0,999 \quad (Б.2)$$

ОПРЕДЕЛЕНИЕ ЦЕННОСТИ ИНФОРМАЦИОННЫХ АКТИВОВ

Ценность актива С определяется стоимостью информационного актива. Так, как невозможно определить точные стоимости активов для организации в целом, рекомендуется ценность актива задавать в диапазоне от 0 до 1, которая будет показывать отношение цены актива к стоимости всего бизнеса. Так, как уровень конфиденциальности сведений, то отношение стоимости активов к стоимости всего бизнеса можно принять 0.5, т.е. С = 0,5.

ОПРЕДЕЛЕНИЕ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ УЯЗВИМОСТЕЙ

Возможность использования организационных уязвимостей проводится экспертным методом, анализируя применяемые организационные меры защиты информации. В ходе проведения анализа, всем организационным мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются (таблица Б.11).

Таблица Б.11 – Коэффициента уязвимости организационных мер ЗИ.

Сумма выполняемых мер защиты	Коэффициент уязвимости (*Ko*)
14–17	0,01
8-13	0,25
Менее 8	0.5
Не выполняются	0,9

В таблице Б.12 представлены соответствие выполняемых организационных мер защиты информации и коэффициент уязвимости организационных мер защиты информации.

Таблица Б.12 – Перечень организационных мер защиты информации реализованных в ООО «ЭНЕРГО»

Организационные меры защиты конфиденциальной документированной информации	Соответст-вия
Ограничение доступа к помещениям, где информация содержится и обрабатывается	0
Установлен режим коммерческой тайны	1

Организационные меры защиты конфиденциальной документированной информации	Соответст-вия
Хранение информации в закрытых для посторонних сейфов	1
Блокировка просмотра содержания обрабатываемых материалов	0
Определение демаскирующих признаков организации и выпускаемой продукции;	0
Организация разработки нормативно-методических документов, разработка проектов распорядительных документов по вопросам организации защиты информации в организации	1
Проведение периодического контроля эффективности мер защиты информации в организации, участие в расследовании нарушений в области ЗИ и разработка предложений по устранению недостатков	0
Организация проведения занятий с руководящим составом и специалистами организации по вопросам защиты информации	1
Наличие перечня сведений являющихся ценными для организации	1
Организация охраны помещений	0
Организации контрольно-пропускных систем на территории организации	1
Установка антивирусного программного обеспечения	1
Систематический контроль уровня защищенности каналов связи	0
Итого	7

Таким образом, коэффициент уязвимости организационных мер защиты информации Ко = 0,5.

Возможность использования технических уязвимостей проводилась экспертным методом, анализируя применяемые технические меры защиты информации. В ходе проведения анализа всем техническим мерам, которые выполняются, присваивается значение «1», в противном случае – «0». Все значения, которым присвоено значение «1», суммируются, остальные значения не учитываются. В таблице Б.13 представлено соответствие выполняемых технических мер защиты информации и коэффициент уязвимости технических мер защиты информации.

Таблица Б.13 – Соответствие выполняемых технических мер защиты информации и коэффициент уязвимости технических мер защиты информации

Сумма выполняемых мер защиты	Коэффициент уязвимости (*Kt*)
15-18	0.01
9-14	0.25
Менее 9	0.5
Не выполняются	0.9

Таблица Б.14 – Перечень технических мер защиты информации реализованных в ООО «ЭНЕРГО»

Технические меры защиты информации	Соответствия
Проверка используемой техники на соответствие величины побочных излучений допустимым уровням;	0
Экранирование помещения с техникой или техники в помещениях;	1
Перемонтированные отдельных цепей, линий, кабелей;	0
Использование специальных устройств и средства пассивной и активной защиты.	1
Разработка рекомендаций по технической защите информации применительно к конкретной организации;	0
Построение комплексных систем защиты информации локальных, глобальных и корпоративных вычислительных сетей	0
Комплексный аудит существующих систем защиты информации в организации	0
Разработка политики безопасности организации	1
Интеграция оборудования и программного обеспечения технической защиты информации в существующую информационную систему организации	1
Установка систем защиты периметра;	1
Разработка пакета внутренней нормативно-методической и распорядительной документации по защите информации ограниченного доступа	1
Оценка защищенности объектов информатизации от утечки по техническим каналам	1
Использование жидкокристаллических или плазменных дисплеев, струйных принтеров и термопринтеров, избегая высокочастотного электромагнитного излучения	0
Минимальная защита снятия информации акустическим способом с помощью мягких прокладок, установленных под оборудованием	1
ИТОГО	8

Расчёты показали, сумма соответствия технических мер защиты информации в ООО «ЭНЕРГО» равно 8, тогда Kt = 0,5.

КОЛИЧЕСТВЕННОЕ ОПРЕДЕЛЕНИЕ РИСКА

В разрабатываемой методике процедура оценки рисков ИБ основывается на взаимности нескольких факторов – вероятности происшествия, а именно вероятности реализации хотя бы одной актуальной угрозы, коэффициента ценности актива, среднеарифметического значения коэффициентов возможности использования организационных уязвимостей и возможности использования технических уязвимостей и

риска несоответствия требованиям законодательства. Под коэффициентом ценности актива понимают ценность или критичность актива по отношению ко всему бизнесу.

Общая формула определения риска ИБ всего перечня актуальных угроз имеет вид:

$$R = P_{угр} * R_n * C * \frac{K_o + K_t}{2} * 100\% , \quad (Б.3)$$

где R – численная величина риска ИБ;

$Pугр$ – вероятность реализации хотя бы одной угрозы из всего перечня угроз;

Rn – риск несоответствия требованиям законодательства;

C – ценность актива (0…1);

Ko – вероятность использования организационных уязвимостей;

Kt – вероятность использования технических уязвимостей.

Проведя расчёты риска ИБ для типов объектов среды влияющих на качество защиты конфиденциальной информации получим:

$$R=0.9999907937*0.5*0.5*(0.5+0.5)/2*100=12.49988492 \quad (Б.4)$$

Допустимый риск принято считать риск, который в данной ситуации считают приемлемым при существующих общественных ценностях. Для предприятий малого и среднего бизнеса рекомендованное значение риска не должно превышать 5%. Это обусловливается в первую очередь тем, что максимальная выручка предприятий МСБ за отчетный период, например 1 год, может составлять до 400 млн рублей, это из расчета того, что в случае реализации одной из актуальных угроз, может повлечь убыток в размере более 5% выручки, является недопустимым и требующим принятия эффективных мер.

Таким образом, можно сделать вывод, что уровень ИБ по всем объектам среды, влияющим на качество защиты конфиденциальной документированной информации ниже допустимого.

Для обеспечения требуемого уровня ИБ для конфиденциальной документированной информации необходимо разработать и реализовать контрмеры для снижения риска ИБ.

ПРИЛОЖЕНИЕ В

(обязательное)

Перечень необходимого оборудования

Таблица В.1 – Перечень необходимого оборудования

Устройство	Назначение	Применение
Сетевое устройство с установленным ПО	Подключение центра управление сетью (ЦУС)	Из комплекта поставки
	Подключение сетевого устройства	Из комплекта поставки
Клавиатура и монитор	Выполнение процедуры инициализации ЦУС	
	Выполнение процедуры инициализации сетевого устройства	
АРМ администратора	Управление сетью КШ	АРМ администратора и сервер БД рекомендуется развертывать на разных компьютерах.
	Управление сервером доступа	
Сервер БД	Хранение регистрационных журналов	
Чистый и отформатированный USB Flash- накопитель	Создание идентификатора администратора комплекса при инициализации ЦУС	Одновременно можно хранить только один ключ ЦУС и один ключ сервера доступа
Чистый и отформатированный USB Flash- накопитель	Создание идентификатора администратора сервера доступа при инициализации сервера доступа	
	Создание единого ключевого носителя для агента ЦУС	
	Запись конфигурации сетевого устройства	
	Запись закрытого ключа центра сертификации при издании корневого сертификата	Можно использовать носитель — идентификатор администратора сервера доступа
	Запись ключей пользователя и сертификата центра сертификации при регистрации удаленного пользователя	

ПРИЛОЖЕНИЕ Г (обязательное) **Сравнительный анализ шлюзов**

Таблица Г.1 – Сравнительный анализ шлюзов [5,11,22]

Характеристики	АПКШ «Континент» 3.7	ПАК ViPNet Coordinator	VPN/FW «ЗАСТАВА» 6.0	Ideco ICS 6.0	ПАК «РУБИКОН - К»	ПАК «ФПСУ-IP/Клиент»	S-terra (Cisco) CSP VPN Gate 3.1
Аппаратные решения	+	+	+	+	+	+	+ (Cisco)
Базовая операционная система	FreeBSD	Адаптированная ОС Linux	ALT Linux 6.0.	Linux	Linux	Linux	Cisco IOS
Интерфейс управления	GUI	веб-интерфейс, графический	графический интерфейс с древовидной	веб-интерфейс, ssh, локальная	веб-интерфейс, графический	графический интерфейс	Cisco Security Management
Требуемое ПО	Windows XP, 2003, Vista, 2008, 7, 8, 8.1 для	Дополнительное не требуется	Дополнительное не требуется	Дополнительное не требуется	Дополнительное не требуется	Дополнительное не требуется	Дополнительное не требуется
Единая консоль управления несколькими	+	+	+	+	+	+	+
ФСТЭК версия	+ СОВ3, МЭ2, НДВ2, НДИ2	+ МЭ3, НДВ3	+ МЭ2, НДВ3,	+ МЭ3, НДВ4	+ МЭ-3, НДВ-4,СОВ-4	+ МЭ5, НДВ4	+ НДВ-3, МЭ-3
Сертифицированная VPN соответствие требованиям ФСБ	+ КС3, МЭ4 (КС1 и КС2) вместе с	+ КС2	+ КС3	+ КС1 и КС2	+ КС1	+ КС1 (на туннель 0)	+ КС1,КС2, КС3

Система предотвращения вторжений (IPS)	+	+	-	+	+	+	+
Межсетевой экран	+	+	+	+	+	+	+
Ограничение количество одновременных	+	+	+	+	+	+	+
Авторизация пользователей Identity-Based	+ специальный клиент	+	+	+ IP/ IP+mac/ логин+пароль	+	+	+
Маршрутизация	+	+	+	+	+	+	+
Резервирование каналов	+	+	-	+	+	+	+
Балансировка каналов	+	+	-	+	+	+	+
Поддержка VLAN	+	+	+	+	+	+	+
Публикация ресурсов	+	+	-	+	-	-	+
QoS и шейпер (контроль полосы пропускания и	+	+	+	+	+	+	+

Шифрование	Шифрование по ГОСТ 28147-89 (256 бит),	Шифрование по ГОСТ 28147-89 (256	ГОСТ 28147-89	AES, Blowfish, Camellia,	ГОСТ 28147-89	ГОСТ 28147-89	ESP_GOST-4M-IMIT (использование
Site-to-site VPN (соединение офисов)	+ ГОСТ-VPN	+ L2TP/IPsec, PPTP	+ IPsec IKEv2, IPsec	+ OpenVPN, IPsec IKEv2,	+ ГОСТ-VPN	+ Собственный (на базе UDP-	IPsec
Client-to-site VPN (подключение клиентов)	+ ГОСТ-VPN	+ L2TP/IPsec, PPTP	+ IPsec IKEv2,	+ L2TP/IPsec, PPTP	+ ГОСТ-VPN	+ Собственный (на базе UDP-	IPsec
DHCP	+	+	+	+	+	+	+
NTP	+	+	+	+	-	+	+
NAT/PAT	+	+	+	+	+	+	+
DNS-сервер	+	-	-	+	-	+	+
SNMP (журналирование)	+	+	+	-	+	+	+
VoIP	+	+	-	-	-	+	+
ADSL	+	+	-	-	-	-	-

Dial-Up	+	+	-	-	-	-	-
Video conference	+	+	-	-	-	-	-
Поддержка внешних 3G-модемов (USB).	+	+	+	-	+	+	+
Защита от DoS атак	+	+	+	+	+	+	+
ЦЕНА на 1 устройство (маршрутизатор	197 340 р	213 800 р	121 300 р	198 000 р	150 000 р	212 400 р	189 300 р