

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Федеральное государственное бюджетное образовательное учреждение
высшего образования

«ПЕНЗЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Политехнический институт
Факультет приборостроения,
информационных технологий и
электроники

Кафедра
«Информационная безопасность
систем и технологий»

Специальность 100503 –

Информационная безопасность
автоматизированных систем

Специализация -

Защищенные автоматизированные
системы управления

ДИПЛОМНАЯ РАБОТА

на тему

МЕТОДИКА ПОСТРОЕНИЯ КОРПОРАТИВНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ
ООО «РОСТОК - МЕБЕЛЬ»

Студент	_____	<u>Вертянов Владислав Александрович</u>
Руководитель	_____	<u>Шумкин С.Н.</u>
Нормоконтролёр	_____	<u>Фатеев А.Г.</u>
Рецензент _____	_____	<u>Лакин К.А.</u>

Работа допущена к защите (протокол заседания кафедры от _____ № _____)

Заведующий кафедрой _____ С.Л. Зефилов

Работа защищена с отметкой _____ (протокол заседания ГЭК
от _____ № _____)

Секретарь ГЭК _____ А.П. Иванов

Пенза 2017

СОДЕРЖАНИЕ:

Обозначения и сокращения.....	5
Введение.....	6
1 Изучение подходов, способов и лучших практик, применяемых для построения комплексной системы защиты информации на промышленных предприятиях	8
2 Анализ существующих методов и средств, применяемых для контроля и защиты информации на предприятии ООО «Росток - мебель», разработка предложений по их совершенствованию и повышению их эффективности ..	13
2.1 Изучение возможностей систем и средств защиты, используемых на предприятии ООО «Росток - мебель»	13
2.2 Разработка предложений по созданию комплексной защиты на предприятии ООО «Росток-мебель»	17
3 Определение угроз безопасности информации на предприятии ООО «Росток-мебель»	19
3.1 Модель нарушителя информационной безопасности ООО «Росток-мебель»	19
3.2 Идентификация рисков информационной безопасности	21
3.2.1 Идентификация и определение ценности активов.....	21
3.2.2 Идентификация угроз безопасности информации на предприятии ООО «Росток - мебель»	31
3.2.3 Идентификация уязвимостей активов автоматизированной системы.	33
3.3 Анализ риска информационной безопасности	37
3.3.1 Оценка последствий	37
3.3.2 Оценка вероятности инцидента	37
3.3.3 Определение уровня риска	38
3.4 Оценивание риска	43
4 Классификация информации в автоматизированной системе предприятия	44

5 Анализ организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ООО «Росток - мебель»	48
5.1 Персональные данные, обрабатываемые в информационных системах персональных данных предприятия ООО «Росток - мебель»	48
5.2 Принципы обработки персональных данных на предприятии ООО «Росток - мебель»	50
5.3 Условия обработки персональных данных на предприятии ООО «Росток - мебель»	51
5.4 Согласие субъекта на обработку персональных данных.....	53
5.5 Доступ к персональным данным	55
5.5.1 Организация внутреннего доступа к персональным данным субъектов персональных данных	55
5.5.2 Предоставление субъекту персональных данных доступа к своим персональным данным.....	56
5.6 Ответственность за нарушение норм, регулирующих обработку и обеспечение безопасности персональных данных	58
5.7 Технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Росток - мебель»	58
5.7.1 Существующие технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Росток - мебель»	58
5.7.2 Требуемые технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Росток - мебель»	61
6 Анализ материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации.	67
6.1 Концепция информационной безопасности ООО «Росток - мебель»	67

6.2 Регламент информационной безопасности ООО «Росток - мебель»	69
6.3 Корпоративная и частные политики информационной безопасности ООО «Росток - мебель»	70
7 Методика построения корпоративной системы защиты информации ООО «Росток - мебель»	72
7.1 Модель построения корпоративной системы защиты информации ООО «Росток - мебель»	72
7.2 Методика построения корпоративной системы защиты информации ООО «Росток - мебель»	75
7.3 Проведение оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений	76
Заключение	78
Список использованных источников	79
Приложение А Структура участка локальной вычислительной сети бухгалтерии.....	81
Приложение Б Структура локальной вычислительной сети предприятия ООО «Росток - мебель»	83
Приложение В Организационная структура предприятия ООО «Росток - мебель»	85

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

PDCA – Plan Do Check Act (планируй делай изучай действуй);
АРМ – автоматизированное рабочее место;
АС - автоматизированная система;
АТС – автоматическая телефонная станция;
БД – база данных;
БС РФ – банковская система Российской Федерации;
ВА – вспомогательные активы;
ДОП – документы общего пользования;
ИА – информационные активы;
ИБ – информационная безопасность;
ИСПДн – информационная система персональных данных;
ИОД – информация ограниченного доступа;
ИТТ – информационные и телекоммуникационные технологии;
КИ – конфиденциальная информация;
НСД – несанкционированный доступ;
ОГКИ – ограниченный доступ к информации;
ПДн – персональные данные;
ПДКИ – полный доступ к информации;
ПО – программное обеспечение;
СЗИ – средства защиты информации;
СИ – секретная информация;
СМИБ – система менеджмента информационной безопасности.

ВВЕДЕНИЕ

С развитием общества, экономики, правовой системы, с их усложнением повышается важность и роль информации. В наше время информация является материалом, работа с которым лежит в основе деятельности многих организаций. Бережное отношение к информации, обеспечение ее максимальной безопасности уже не просто блажь, а это необходимость, продиктованная ритмами и качеством современной жизни. Безопасность информации является тем фактором, от которого во многих случаях зависит благополучие организации, ее сотрудников и клиентов. Организации, сфера деятельности которых лежит в области работы с поступающей к ним информацией, должны надлежащим образом следить за ее получением, формированием, хранением, обработкой, распределением и использованием. Должен быть исключен доступ посторонних лиц к конфиденциальной информации, так как несанкционированный доступ к такой информации может привести к неблагоприятным последствиям в деятельности организации. Для полного исключения подобных случаев, необходимо осуществлять контроль над информационной системой, поддерживать обеспечение информационной безопасности (далее ИБ).

Неудивительно, что подавляющее большинство лиц, ответственных за обеспечение ИБ, неоднократно пыталось понять, как максимально качественно произвести оценку уровня защищенности информационных активов организации, а также выяснить перспективы развития системы защиты информации.

На данный момент существуют современные методики, применяемые в управлении рисками, проектировании и сопровождении корпоративных систем защиты информации, которые способствуют решению ряда задач стратегического перспективного развития компании, а именно:

- количественной оценке текущего уровня информационной безопасности компании, для чего требуется выявление рисков на

техническом, технологическом, организационно-управленческом и правовом уровнях обеспечения информационной защиты;

- разработке и реализации комплексного плана модернизации корпоративных систем защиты информации, чтобы обеспечить защищенность информационных активов компании на приемлемом уровне.

Чтобы реализовать данную задачу, необходимы следующие шаги:

- обоснование и произведение расчета финансовых вложений в безопасность основываясь на технологиях анализа рисков, соотнесение расходов на обеспечение безопасности и потенциального ущерба, а также вероятности его возникновения;

- выявление и проведение первоочередного блокирования наиболее опасных уязвимостей до того, как уязвимые ресурсы будут атакованы;

- определение функциональных отношений и зон ответственности в ходе взаимодействия подразделений и лиц, связанного с обеспечением информационной безопасности компании, создание необходимого пакета организационно-распорядительных документов;

- разработка и согласование с надзорными органами и со службами организации проекта внедрения необходимых комплексов защиты, учитывающих тенденции развития и современный уровень информационных технологий;

- обеспечение поддержания внедренных комплексов защиты, согласно изменяющимся условиям работы организации, регулярным доработкам организационно-распорядительной документации, модернизации технических средств защиты, модификации технологических процессов.

1 Изучение подходов, способов и лучших практик, применяемых для построения комплексной системы защиты информации на промышленных предприятиях

Не секрет, что у каждого предприятия есть своя основная задача, например, производство продукции и получение прибыли от ее реализации. Практические всегда, построение комплексной защиты информации не входит в перечень основных задач ни одного предприятия. Тем не менее, это крайне важная часть успешного функционирования любого предприятия. Именно в силу второстепенности построения комплексной системы защиты информации (далее, СЗИ) относительно главных задач организации, она не должна быть причиной ощутимых трудностей в работе компании, и в то же время, создание СЗИ должно быть экономически оправданным. При всем при этом, она должна обеспечить необходимую защиту важных информационных ресурсов организации от всевозможных угроз.

Существует точка зрения, согласно которой, проблемы защиты информации имеют отношение только к той информации, которую обрабатывает компьютер. Данное мнение основывается на том, что компьютеры, и в частности персональные компьютеры, являются центрами хранения информации. Однако, по нашему мнению, объект информатизации, в отношении которых направлены действия, связанные с защитой информации, является куда более широким и многообразным, нежели персональный компьютер.

В соответствии с ГОСТ Р 51275-99 [3] под объектом информатизации понимается совокупность информационных ресурсов, систем и средств обработки информации, которые используются согласно заданной информационной технологии, средств обеспечения объекта информатизации, помещений или объектов (зданий, сооружений, технических средств), в которых они установлены, или помещения и объекты, предназначенные для ведения конфиденциальных переговоров.

Из указанного определения объекта информации можно сделать заключение о том, что слово «совокупность» подразумевает, что объект информатизации является единой информационной системой, охватывающей в целом учреждение, предприятие, организацию.

В соответствии с ГОСТ Р ИСО/МЭК 27001-2006 [4] устанавливаются требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (далее, СМИБ) среди общих коммерческих рисков организации. Кроме того, устанавливаются требования по внедрению мер управления ИБ и ее контроля, которые могут быть использованы организациями или их структурными подразделениями в соответствии с целями и задачами обеспечения ИБ. Указанный стандарт применяется организациями всех форм собственности.

Необходимо отметить, что целью построения СМИБ является выбрать соответствующие меры управления безопасностью, предназначенные для того, чтобы защитить информационные активы и гарантировать доверие заинтересованных сторон.

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СМИБ применительно ко всей деловой деятельности организации. С учетом целей рассматриваемого стандарта используемый процесс основан на применении модели PDCA, приведенной на рисунке 1.

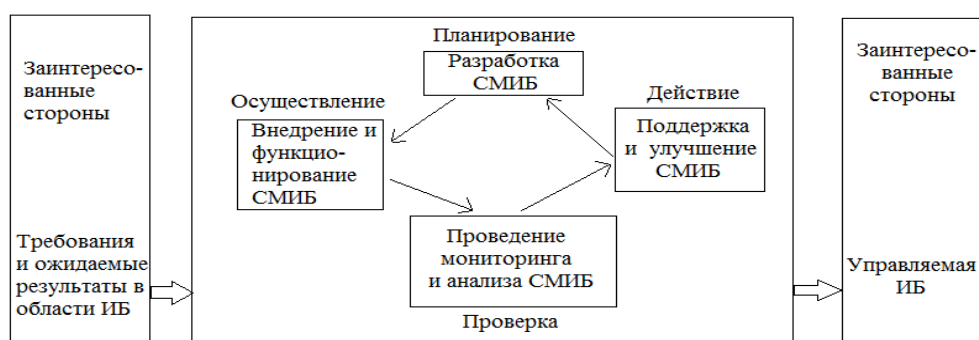


Рисунок 1 – Модель PDCA

Указанный стандарт является руководством по управлению безопасностью информационных и телекоммуникационных технологий (далее, ИТТ), устанавливает концепцию и модели, лежащие в основе базового понимания безопасности ИТТ, а также раскрывает общие вопросы управления, важные, чтобы успешно планировать, реализовывать, и поддерживать безопасность ИТТ. Целью настоящего стандарта является сформировать общие понятия и модели управления безопасностью ИТТ. Положения, которые приведены в нём, обладают общим характером и могут быть применены к самым разным организациям и методам управления. Указанный стандарт [4] применяется таким образом, что допустимо приспособление его положений к потребностям организаций и свойственным им стилям управления. Данный стандарт не включает конкретные подходы к управлению безопасностью.

Таким образом, комплексная система защиты информации на промышленных предприятиях призвана защищать активы как снаружи, так и изнутри.

Способы защиты предприятия изнутри – включают комплекс информационной безопасности и систему мониторинга за персоналом. Как правило, данные средства состоят из следующих компонентов:

- средств скрытого видеоконтроля. Применяются разные камеры. От обзорных, в том числе, работающих в инфракрасном диапазоне, до узкоугольных камер высокого разрешения, позволяющих фиксировать документы или психологические реакции в ходе деловых переговоров. Телекамеры можно камуфлировать в любой предмет интерьера: датчик охранной сигнализации, картину, настенные часы и т.п;
- средств контроля над акустической обстановкой в помещении. Применяются, чтобы отслеживать различные переговоры;
- средств контроля над телефонными переговорами, включая факсимильные сообщения. Применяется оборудование разных типов и характеристик, в зависимости от того, АТС какого типа установлена на

объекте. У каждого типа цифровой учрежденческой АТС есть собственный закрытый протокол связи. Впрочем, для современных технологий это не составляет проблемы;

- средств защиты информационных ресурсов сетей и компьютеров, в том числе, контроль интернет-трафика и сетевого трафика;
- мониторинга радиозэфира. Применяется, чтобы избежать утечек информации, при которых транспорт сигнала производился бы по радиоканалу;
- средств парирования утечек конфиденциальной информации через различные физические каналы - комплексов локализации и подавления подслушивающих устройств.

Всесторонний анализ состояния защищенности информационных ресурсов предприятия, при учёте стремления конкурентов к захвату конфиденциальной информации и, тем самым, нанесению вреда предприятию является одним из важнейших подходов к созданию СЗИ. Необходимо отметить, что основополагающим элементом анализа следует назвать работу, связанную с определением перечня защищаемых информационных ресурсов, учитывающего особенности их расположения (размещения) и доступа к данным ресурсам разных категорий работников (сотрудников иных предприятий).

Руководитель организации и его заместитель непосредственно возглавляют работу по проведению такого анализа, что говорит о ее важности для предприятия. Любой опыт работы организации, будь то положительный или отрицательный, накопленный в течение нескольких лет является основой для изучения защищенности информационных ресурсов. Кроме того, основой для такого изучения являются и деловые связи, а также контакты предприятия, осуществляющие аналогичные виды деятельности.

При построении комплексной СЗИ, в прежде всего, необходимо учесть особенно важные направления работы предприятия, которые требуют особого внимания. Кроме того, приоритет также получают новые,

перспективные направления работы предприятия, связанные с такими аспектами его работы, как научные исследования, новейшие технологии, формирующие интеллектуальную собственность, а также развивающиеся международные связи. Согласно названным приоритетам, формируют список вероятных угроз информации, которая подлежит защите, и определяют конкретные средства, силы, методы и способы ее защиты.

Система защиты информации должна обладать следующими признаками:

- централизованность, позволяющая обеспечивать результативное управление системой со стороны руководителей и должностных лиц, которые отвечают за разнообразные направления работы организации;
- плановость, позволяющая объединить действия разных должностных лиц и структур, чтобы выполнить стоящие перед организацией задачи в области защиты информации;
- конкретность и целенаправленность, рассчитанные на то, чтобы защитить абсолютно конкретные информационные ресурсы, которые представляют интерес для конкурентов;
- активность, обеспечивающая защиту информации при достаточной степени настойчивости и возможности концентрации усилий на особенно значимых направлениях работы организации;
- надежность и универсальность, охватывающие всю деятельность предприятия, связанную с созданием и обменом информацией.

2 Анализ существующих методов и средств, применяемых для контроля и защиты информации на предприятии ООО «Росток - мебель», разработка предложений по их совершенствованию и повышению их эффективности

2.1 Изучение возможностей систем и средств защиты, используемых на предприятии ООО «Росток - мебель»

Средства защиты информации представляет собой комплекс устройств и приспособлений, приборов и технических систем (инженерно-технические, электрические, электронные, оптические и другие), а также прочих вещных элементов, которые используются, чтобы решать различные задачи, связанные с защитой информации, включая упреждение утечек и обеспечение безопасности защищаемой информации.

В соответствии со стандартами Банка России СТО БР ИББС-1. 1-2007 [5] основной вид проверки уровня ИБ в организациях БС РФ представляет собой аудит ИБ. В соответствии с мировым опытом в области обеспечения ИБ, аудит ИБ определяется в качестве важнейшего процесса в непрерывных циклах процессов менеджмента ИБ организаций. Банк России – сторонник регулярных аудитов ИБ в организациях БС РФ. Основные цели аудитов ИБ организаций БС РФ заключаются:

- в повышении доверия к организациям, входящим в БС РФ;
- в оценке соответствия ИБ организаций, входящих в БС РФ, критериям, которые предъявляет аудит ИБ.

В данном стандарте, под термином аудитор (эксперт), понимается лицо, которое обладает компетентностью, чтобы проводить аудит информационной безопасности.

Следует выделить главные принципы, в соответствии с которыми проводится аудит информационной безопасности организаций, входящих в БС РФ:

- независимый характер аудита ИБ. Аудиторы являются независимыми в их деятельности и не несут ответственности за деятельность, которую подвергают аудиту ИБ. Независимость – это основание для

беспристрастности в ходе проведения аудита ИБ и объективности, в ходе формирования заключений по результатам аудитов ИБ;

- полнота аудита ИБ. Данный аудит обязан охватить все области аудита ИБ, которые соответствуют заданию аудиторов. Полноту аудита ИБ следует расценивать, как необходимое условие, чтобы сформировать объективные заключения по результатам, полученным при аудите ИБ;

- оценка, основанная на аудите ИБ. В случае периодического проведения аудита ИБ, оценку, основанную на свидетельствах аудита ИБ следует принимать, как единственный способ, позволяющий получить повторяемые заключения по результатам аудита ИБ. Чтобы заключения были повторяемыми, свидетельства аудита быть проверяемыми;

- достоверность свидетельств, полученных при аудите ИБ. Аудиторы должны быть уверены в том, что свидетельства аудита ИБ достоверны. Для повышения доверия к документальным свидетельствам аудитов ИБ, достоверность данных аудитов должна быть подтверждена третьей стороной или же руководством организации, которая входит в БС РФ;

- компетентность. Доверие к процессу и результатам аудита ИБ зависит от компетентности тех, кто проводит аудит ИБ, и от этичности их поведения. Компетентность базируется на способности аудитора применять знания и навыки;

- этичность поведения. Этичность поведения подразумевает ответственность, неподкупность, умение хранить тайну, беспристрастность.

Таким образом, в ходе проведения аудита информационной безопасности на предприятии ООО «Росток - мебель» было проанализировано наличие и текущее состояние средств защиты информации, анализ проводился по следующим направлениям:

- организационно-распорядительная документация;

- наличие на предприятии области документов, касающихся защиты информации;
- защита зданий и помещений;
- защита автоматизированной системы.

В результате проведенного анализа было выявлено, что на предприятии ООО «Росток - мебель» существуют меры по защите информации, а также на данном предприятии используются как программные, так и аппаратные средства защиты информации.

Аппаратные средства это различные по типу устройства (механические, электромеханические, электронные и др.), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникновению, либо, если проникновение все же состоялось, доступу к информации, в том числе с помощью ее маскировки. Первую часть задачи решают замки, решетки на окнах, защитная сигнализация и др. Вторую - генераторы шума, сетевые фильтры, сканирующие радиоприемники и множество других устройств, "перекрывающих" потенциальные каналы утечки информации или позволяющих их обнаружить. Преимущества аппаратных средств связаны с их надежностью, независимостью от субъективных факторов, высокой устойчивостью к модификации. Слабые стороны – недостаточная гибкость, относительно большие объем и масса, высокая стоимость.

Организационно-распорядительные меры:

- корпоративная политика предприятия;
- инструкция по делопроизводству;
- наличие в штате службы безопасности.

Защита зданий и помещений:

- металлический забор вокруг здания;
- железные ворота на въездах;
- наличие металлических решеток на окнах;
- наружные металлические двери;

- наличие в кабинетах железных шкафов.

Защита автоматизированной системы:

- антивирусное программное обеспечение Kaspersky Internet Security 2015;
- источники бесперебойного электропитания АРМ.

Программные средства включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др. Можно выделить следующие преимущества программных средств – универсальность, гибкость, надежность, простота установки, способность к модификации и развитию. К недостаткам программных средств следует отнести – ограниченную функциональность сети, использование части ресурсов файл-сервера и рабочих станций, высокую чувствительность к случайным или преднамеренным изменениям, возможную зависимость от типов компьютеров (их аппаратных средств).

В состав программных средств защиты информации входят:

- средства антивирусной защиты, такие как: Kaspersky Endpoint Security Стандартный;
- система доменов «Unix» и «Windows», а также рабочие группы.

Как видно из представленных выше защитных мер, на предприятии отсутствует комплексная система защиты информации, а представлены лишь отдельные средства и методы защиты.

При доработке комплексной системы защиты информации целесообразно будет усилить персональный фаервол, который сам контролирует сетевой трафик и не позволяет злоумышленникам проникнуть в компьютер. Так же будет правильно применять на ПК такие СЗИ от НСД как Secret Net и Secret Net LSP, которые позволяют успешно решать стоящие перед организацией задачи разграничения доступа к информации, контроля устройств и потоков конфиденциальных данных.

2.2 Разработка предложений по созданию комплексной защиты на предприятии ООО «Росток-мебель»

Организационное мероприятие - это мероприятие направленное на защиту информации, проведение которого не требует применения специально разработанных технических средств.

Перечень необходимых организационных мероприятий по защите информации:

- создание подразделений по защите информации в организации;
- назначить штатного специалиста по защите информации;
- разработать должностные инструкции сотрудников;
- назначить ответственные лица за обеспечение защиты информации на отдельных объектах и подразделениях организации;
- обозначит обязанности и права должностных лиц организации, ответственных за разработку, обеспечения выполняемых мероприятий на объектах и подразделениях;
- установить форму документирования результатов аттестации и порядок выдачи разрешения на проведение работ с секретной информацией, а также порядок и периодичность продления аттестата;
- провести аттестацию помещений организации;
- все аттестационные помещения утвердить приказом директора организации;
- на каждое помещение оформить аттестационный паспорт;
- разработать план финансирования мероприятий по защите информации в организации;
- определить исполнение работ по защите информации.

На этапе организационных мероприятий проводятся:

- установление границ и размеров контролируемой зоны, в которой исключено пребывание посторонних лиц;

- выявления наличия и состава средств слаботочной техники в контролируемой зоне;
- уточнение назначения и необходимости применения средств слаботочного оборудования в производственных и управленческих звеньях; выявление технических средств, применение которых служебной необходимостью не обосновано;
- выявление наличия задействованных и незадействованных воздушных, наземных, подземных, настенных, а также заложенных в скрытую канализацию кабелей и проводов, уходящих за пределы контролируемой зоны;
- уточнение перечня режимных помещений, в которых проводятся или должны проводиться закрытые мероприятия постоянного или временного характера (обмен мнениями, обсуждения, беседы, совещания и др.);
- выявление наличия в режимных помещениях оконечных устройств слаботочного оборудования; уточнение перечня помещений, в которых сосредотачиваются технические средства, предназначенные для обслуживания режимных помещений.

3 Определение угроз безопасности информации на предприятии ООО «Росток-мебель»

3.1 Модель нарушителя информационной безопасности ООО «Росток-мебель»

Для того чтобы определить актуальные угрозы безопасности информации для автоматизированной системы предприятия ООО «Росток-мебель» необходимо иметь представление о возможном нарушителе, то есть необходимо составить модель нарушителя, а также идентифицировать риски информационной безопасности и идентифицировать информационные активы и определить их ценности.

Модель вероятного нарушителя безопасности ИС необходима для систематизации информации о типах и возможностях субъектов, целях несанкционированных воздействий и выработки адекватных организационных и технических мер противодействия.

При разработке модели нарушителя ИС учитываются:

- предположения о категориях лиц, к которым может принадлежать нарушитель; тип нарушителя;
- предположения о мотивах действий нарушителя (преследуемых нарушителем целях);
- предположения о квалификации нарушителя и его технической оснащенности (об используемых для совершения нарушения методах и средствах);
- ограничения и предположения о характере возможных действий нарушителей;
- характер информационных угроз.

По наличию права разового или постоянного доступа нарушители делятся на два типа: нарушители, которые используют внешние угрозы и нарушители, которые имеют доступ к ИС и используют внутренние угрозы.

В таблице 1 приведены категории лиц, которые могут использовать внутренние или внешние угрозы.

Таблица 1 – Перечень лиц, которые могут использовать внутренние или внешние угрозы

Тип нарушителя	Категория лиц
Внешний	Разведывательные службы государств; криминальные структуры; представители конкурирующих организаций (иностранных спецслужб) или лица, действующие по их заданию; недобросовестные партнеры; клиенты (представители организаций, граждане); посетители (приглашенные по какому-либо поводу); представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжения и т.п.); лица, случайно или умышленно нарушившие пропускной режим; любые лица за пределами контролируемой территории.
Внутренний	Пользователи ИС; администраторы ИС; персонал, обслуживающий технические средства (инженеры, техники); сотрудники отделов; технический персонал, обслуживающий здания (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здания и помещения); сотрудники службы безопасности; руководители различных уровней должностной иерархии.

3.2 Идентификация рисков информационной безопасности

3.2.1 Идентификация и определение ценности активов

Информационные активы — те активы, которые необходимы для деятельности бизнес-организации, активы, которые имеют высокую стоимость или сбор, хранение, обработка и передача которых требует продолжительного времени или связана с большими затратами на приобретение.

Различают основные и вспомогательные активы. К основным активам относятся бизнес-процессы и информационные активы в области применения управления рисками.

Были идентифицированы информационные активы предприятия ООО «Росток-мебель», их форма хранения, также было определено какие из свойств ИБ для этих информационных активов являются значимыми.

Перечень информационных активов и их значимых свойств ИБ представлен в таблице 2, где значимое свойство ИБ для информационного актива обозначается знаком «+», незначимое – знаком «-».

Таблица 2 – Перечень информационных активов предприятия ООО «Росток-мебель» и их значимых свойств ИБ

Информационный актив	Значимые свойства информационной безопасности		
	Конфиденциальность	Целостность	Доступность
ИА1 - Нормативная и правовая документация	-	+	+
ИА2 - Устав организации	-	+	+
ИА3 - Техническая документация	-	+	-
ИА4 - Должностные инструкции	—	+	+
ИА5 - Отчетность бухгалтерии	+	+	-
ИА6 - Отчетность отдела ИБ	+	+	+
ИА7 - Персональные данные	+	+	+
ИА8 - Приказы и постановления директора	+	+	+

Продолжение таблицы 2

Информационный актив	Значимые свойства информационной безопасности		
	Конфиденциальность	Целостность	Доступность
ИА9 – Информация о продукции и услугах	-	+	+
ИА10 - Договор об оказании услуг	+	+	+
ИА11 – Отчетная документация отдела маркетинга сбыта и информации	+	+	+
ИА12 - Отчетность отдела работы с клиентами	+	+	-
ИА13 – Отчетная документация планово-экономического отдела	+	+	+
ИА14 – Отчетная документация отдела внешней комплектации и снабжения	+	+	+

Далее для каждого значимого свойства каждого информационного актива предприятия ООО «Росток-мебель» была определена величина нарушения ИБ в соответствии со следующей качественной шкалой:

- минимальная;
- не значительная;
- средняя;
- высокая;
- критическая.

Величина потенциального ущерба от нарушения свойств ИБ активов была оценена по следующим направлениям:

- степень влияния на непрерывность деятельности организации (направление 1);

– объем финансовых и материальных затрат, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ (направление 2);

– объем дополнительных людских ресурсов, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ (направление 3);

– объем дополнительных временных затрат, необходимых для восстановления свойств ИБ для информационного актива и ликвидации последствий нарушения ИБ (направление 4);

– степень нарушения законодательных требований и(или) договорных обязательств организации (направление 5).

Оценка величины нарушения ИБ была выполнена по каждому из указанных выше направлений.

Критерии, по которым определялась величина нарушения ИБ по направлению 1, приведены в таблице 3.

Таблица 3 – Критерии определения величины нарушения ИБ в соответствии со степенью влияния на непрерывность деятельности организации

Величина нарушения ИБ	Критерии определяющие величину нарушения ИБ
Минимальная	Нарушение процессов деятельности, в которых задействован информационный актив, не происходит.
Не значительная	Возможны не значительные нарушения процесса деятельности, в которых задействован информационный актив.
Средняя	Возможно нарушение процессов деятельности, в которых задействован информационный актив. Виды основной деятельности организации, в рамках которых функционируют указанные процессы, не нарушаются.
Высокая	Возможно нарушение процессов деятельности, в которых задействован информационный актив. Возможно нарушение некоторых видов основной деятельности организации, реализуемым данными процессами.

Продолжение таблицы 3

Величина нарушения ИБ	Критерии определяющие величину нарушения ИБ
Критическая	Возможно нарушение процессов деятельности, в которых задействован информационный актив. Возможно нарушение основной деятельности подразделений организации или организации в целом.

Критерии, определяющие величину нарушения ИБ по направлению 2 приведены в таблице 4.

Таблица 4 – Критерии определения нарушения ИБ в соответствии с объемом необходимых финансовых и материальных затрат

Величина нарушения ИБ	Критерии определяющие величину нарушения ИБ
Минимальная	Для восстановления свойств ИБ информационного актива и ликвидации последствий нарушения ИБ финансовые и материальные затраты не требуются.
Не значительная	Для восстановления свойств ИБ информационного актива и ликвидации последствий нарушения ИБ могут потребоваться минимальные финансовые и материальные затраты.
Средняя	Для восстановления свойств ИБ информационного актива и ликвидации последствий нарушения ИБ могут потребоваться финансовые и материальные затраты, планируемые в рамках бюджета организации для ликвидации подобных нарушений.
Высокая	Для восстановления свойств ИБ информационного актива и ликвидации последствий нарушения ИБ могут потребоваться сверхплановые финансовые и материальные затраты из бюджета организации.
Критическая	Для восстановления свойств ИБ информационного актива и ликвидации последствий нарушения ИБ могут потребоваться сверхплановые финансовые и материальные затраты, объем которых не может быть покрыт бюджетом организации, вследствие чего потребуется привлечение финансовых и материальных средств со стороны.

Критерии, определяющие величину нарушения ИБ по направлению 3 приведены в таблице 5.

Таблица 5 – Критерии определения нарушения ИБ в соответствии с объемом дополнительных людских ресурсов

Величина нарушения ИБ	Критерии определяющие величину нарушения ИБ
Минимальная	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может быть осуществлено сотрудниками организации в рамках своих должностных обязанностей.
Не значительная	Восстановление свойств ИБ информационного актива и ликвидация последствий нарушения ИБ может быть осуществлено сотрудниками организации в рамках своих должностных обязанностей.
Средняя	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может потребовать привлечение сотрудников организации, действующих вне рамок своих должностных обязанностей, но обладающих компетенцией и квалификацией для выполнения подобной деятельности.
Высокая	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может потребовать привлечение сотрудников организации, действующих вне рамок своих должностных обязанностей и не обладающих компетенцией и квалификацией для выполнения подобной деятельности.
Критическая	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может потребовать привлечение сотрудников сторонних организаций.

Критерии, определяющие величину нарушения ИБ по направлению 4 приведены в таблице 6.

Таблица 6 – Критерии определения нарушения ИБ в соответствии с объемом дополнительных временных затрат

Величина нарушения ИБ	Критерии определяющие величину нарушения ИБ
Минимальная	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может быть осуществлено всеми сотрудниками организации.
Не значительная	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может быть осуществлено сотрудниками организации в рамках своей основной деятельности.
Средняя	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может потребовать дополнительных временных затрат от сотрудников организации, объем которых не наносит ущерба их основной деятельности.
Высокая	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может потребовать дополнительных временных затрат от сотрудников организации, объем которых нанесет ущерб их основной деятельности.
Критическая	Восстановление свойств ИБ информационного актива и ликвидация последствия нарушения ИБ может потребовать дополнительных временных затрат от сотрудников организации, объем которых прервет их основную деятельность.

Критерии, определяющие величину нарушения ИБ по направлению 5 приведены в таблице 7.

Таблица 7 – Критерии определения нарушения ИБ в соответствии со степенью нарушения законодательных требований и(или) договорных обязательств

Величина нарушения ИБ	Критерии определяющие величину нарушения ИБ
Минимальная	Нарушение свойства ИБ информационного актива не приводит к нарушению законодательных требований и(или) договорных обязательств.
Не значительная	Нарушение свойства ИБ информационного актива приводит к минимальному нарушению законодательных требований и(или) договорных обязательств.
Средняя	Нарушение свойства ИБ информационного актива приводит к нарушению законодательных требований и(или) договорных обязательств, в результате чего к сотрудникам организации могут быть применены дисциплинарные и(или) материальные меры наказания.
Высокая	Нарушение свойства ИБ информационного актива приводит к нарушению законодательных требований и(или) договорных обязательств, в результате чего возможны судебные разбирательства и к сотрудникам организации могут быть применены административные меры наказания.
Критическая	Нарушение свойства ИБ информационного актива приводит к нарушению законодательных требований и(или) договорных обязательств, в результате чего возможны судебные разбирательства и к сотрудникам организации могут быть применены уголовные меры наказания.

Результаты оценивания величины нарушения ИБ для каждого информационного актива по всем пяти направлениям представлены в таблице 8. Также в этой таблице представлена обобщённая качественная оценка величины нарушения ИБ.

Таблица 8 - Результат оценивания величин нарушения ИБ

Информационный актив	Свойства безопасности	Величины нарушения ИБ по направлениям оценивания					Обобщённая величина нарушения ИБ	Ценность актива
		1	2	3	4	5		
Нормативная и правовая документация	Целостность	С	С	Н	С	С	С	С
	Доступность	С	М	Н	С	С	С	
Устав организации	Целостность	М	М	Н	С	С	С	С
	Доступность	М	М	Н	С	С	С	
Техническая документация	Целостность	В	С	В	К	С	К	К
Должностные инструкции	Целостность	В	С	М	С	М	В	В
	Доступность	В	С	М	С	М	В	
Отчетность бухгалтерии	Конфиденциальность	С	С	С	В	В	В	К
	Целостность	В	В	М	К	К	К	
Отчетность отдела ИБ	Конфиденциальность	С	В	М	В	С	В	В
	Целостность	М	С	С	В	С	С	
	Доступность	М	С	С	В	С	С	
Персональные данные	Конфиденциальность	К	К	М	С	В	К	К
	Целостность	В	С	С	С	В	В	
	Доступность	В	С	С	С	В	В	
Приказы и постановления директора	Конфиденциальность	Н	С	С	М	М	С	В
	Целостность	В	М	С	С	В	В	
	Доступность	С	М	М	М	С	С	
Информация о продукции и услугах	Целостность	К	К	С	В	С	В	В
	Доступность	С	В	М	С	С	В	
Договор об оказании услуг	Конфиденциальность	В	К	М	К	В	К	К
	Целостность	С	В	С	К	В	К	
	Доступность	В	В	С	Н	Н	В	
Отчетная документация отдела маркетинга сбыта и информации	Конфиденциальность	С	В	М	С	М	В	В
	Целостность	С	С	М	В	М	В	
	Доступность	М	С	С	М	М	С	
Отчетность отдела работы с клиентами	Конфиденциальность	М	С	С	В	В	В	К
	Целостность	С	В	М	К	К	К	
Отчетная документация планово-экономического отдела	Конфиденциальность	В	С	М	С	С	В	В
	Целостность	С	С	Н	С	М	С	
	Доступность	С	С	Н	М	М	С	
Отчетная документация отдела внешней комплектации	Конфиденциальность	С	Н	С	С	М	С	С
	Целостность	С	Н	С	М	С	С	
	Доступность	С	М	С	М	С	С	

Вспомогательные активы - это аппаратные и программные средства, коммуникационное оборудование, персонал и пользователи. Основные активы зависят от вспомогательных.

Поэтому была определена целостность вспомогательных активов на основе их стоимости, а также ценности зависимых от них информационных активов. Критерии, по которым проводилось оценивание стоимости вспомогательных активов, приведены в таблице 9.

Таблица 9 – Критерии определения стоимости вспомогательных активов

Стоимость	Критерии, определяющие величину стоимости
Минимальная	Затраты на приобретение и поддержку актива составляют незначительную часть бюджета организации. Дополнительные средства для их восстановления не требуются.
Средняя	Затраты на приобретение и поддержку актива составляют существенную часть бюджета организации. Для восстановления поврежденного актива могут потребоваться дополнительные средства, планируемые в рамках бюджета организации для ликвидации подобных повреждений.
Высокая	Затраты на приобретение и поддержку актива составляют большую часть бюджета организации. Для восстановления поврежденного актива могут потребоваться сверхплановые финансовые и материальные затраты из бюджета организации
Критическая	Затраты на приобретение и поддержку актива составляют большую часть бюджета организации. Для восстановления поврежденного актива могут потребоваться сверхплановые финансовые и материальные затраты, объем которых не может быть покрыт бюджетом организации, вследствие чего потребуется привлечение финансовых и материальных средств со стороны.

Оценка ценности вспомогательных активов представлена в таблице 10.

Таблица 10 - Ценность вспомогательных активов

Обозначение	Наименование	Количество	Ценность актива
BA1	Внутренний сервер организации	1	В
BA2	Сервер	1	В
BA3	АРМ системного администратора	1	В
BA4	АРМ генерального директора	1	С

Продолжение таблицы 10

Обозначение	Наименование	Количество	Ценность актива
BA5	АРМ заместителя генерального директора	1	В
BA6	АРМ сотрудников отдела работы с клиентами	5	В
BA7	АРМ сотрудников отдела планово-экономического отдела	1	С
BA8	АРМ сотрудников отдела маркетинга сбыта и информации	1	С
BA9	АРМ сотрудников отдела кадров	1	С
BA10	АРМ сотрудников отдела внешней комплектации и снабжения	3	С
BA11	АРМ сотрудников отдела бухгалтерии	3	С
BA12	Периферийное оборудование	10	С
BA13	Прикладное ПО	10	С

Ценность активов, от которых зависят другие активы, определялась следующим образом:

- если ценность зависимых активов ниже или равна ценности рассматриваемого актива), его ценность остается такой же;
- если ценность зависимых активов больше ценности рассматриваемого актива, его ценность должна быть увеличена.

Зависимости между активами представлены в таблице 11.

Таблица 11 – Матрица зависимостей между активами

Зависимый актив	Актив												
	BA1	BA2	BA3	BA4	BA5	BA6	BA7	BA8	BA9	BA10	BA11	BA12	BA13
ИА1	+	+	+	+	+	-	+	+	-	-	-	-	-
ИА2	+	+	+	+	+	-	+	+	-	-	-	-	-
ИА3	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА4	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА5	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА6	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА7	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА8	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА9	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА10	-	-	-	-	-	-	-	-	-	-	-	-	-

Продолжение таблицы 11

Зависимый актив	Актив												
	BA1	BA2	BA3	BA4	BA5	BA6	BA7	BA8	BA9	BA10	BA11	BA12	BA13
ИА11	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА12	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА13	-	-	-	-	-	-	-	-	-	-	-	-	-
ИА14	+	+	+	+	+	-	-	+	-	-	-	-	-

3.2.2 Идентификация угроз безопасности информации на предприятии ООО «Росток - мебель»

На данном этапе выполнения дипломной работы в соответствии с ГОСТ Р ИСО/МЭК 27005-2010 [6] была проведена идентификация угроз информационной безопасности предприятия ООО «Росток - мебель».

Цель процесса – определение актуальных угроз и оценка возможности их реализации.

Угроза ИБ — совокупность условий и факторов, создающих опасность нанесения ущерба объекту вследствие нарушения свойств ИБ.

Угрозы могут быть:

- по происхождению:
 - природные;
 - антропогенные;
 - техногенные;
- по отношению к объекту:
 - внутренние;
 - внешние;
 - случайные;
 - умышленные.

Информация для идентификации и оценка вероятности угроз может быть получена от владельца актива, пользователей, руководства организации, специалиста по ИБ, а также из других источников (реестр угроз).

Для определения актуальности угроз на предприятии ООО «Росток-мебель» следует установить соответствие между активами и угрозами, которые приводят к нарушению свойств ИБ активов. Существование такого соответствия указывает на актуальность рассматриваемой угрозы.

Угрозы, актуальные для системы, с указанием их источника, целей, и типов потерь представлены в таблице 12.

События обозначаются следующим образом:

- У – преднамеренные события (определяют все преднамеренные действия, которые нацелены на активы АС);
- С – случайные события (определяют все случайные действия, которые нацелены на активы АС);
- П – события среды (определяют все инциденты, которые не основаны на действиях человека).

Таблица 12 – Угрозы, актуальные для системы

Угроза	Тип событий	Источник угрозы	Тип потерь
У1 - Нарушение функционирования технических средств обработки информации	У, С	сотрудники, инсайдеры	Ц, Д
У2 - Нарушение функционирования программного обеспечения	У, С	сотрудники, инсайдеры, хакеры	Д
У3 - Использование контрафактного или скопированного программного обеспечения	У, П	сотрудники, системный администратор	Ц
У4 - Разглашение информации лицам, не имеющим права доступа к защищаемой информации	У, П	сотрудники, инсайдеры	К
У5 - Установка нелицензионного ПО	У, П	сотрудники, системный администратор, хакеры	Ц
У6 - Несоблюдение требований по защите информации	У, П	сотрудники, системный администратор	К, Ц

Продолжение таблицы 12

Угроза	Тип событий	Источник угрозы	Тип потерь
У7 - Ошибки при эксплуатации средств и систем ЗИ	У, П	сотрудники	К, Ц, Д
У8 - Отказы и аварии систем обеспечения объекта информатизации	У, С, П	инсайдеры	Д
У9 – Отказ сетевого оборудования	У, С	инсайдеры, хакеры	Д
У10 - Заражение компьютерными вирусами через съёмные носители информации, компьютерную сеть, сеть Интернет	У, С	сотрудники, инсайдеры, хакеры	К, Ц
У11- Ошибки штатных сотрудников (неверный ввод данных или изменение данных)	П	сотрудники	Ц, Д
У12 - Угрозы целостности баз данных	У, С	сотрудники, системный администратор, инсайдеры	Ц
У13 - Кража оборудования	У	сотрудники, инсайдеры	К, Ц, Д
У14 - Делегирование лишних или неиспользуемых полномочий на носитель с конфиденциальной информацией	У, С	сотрудники, системный администратор	К
У15 - Пожар	У, С, П	сотрудники, природные явления	К, Ц, Д
У16 - Нарушение энергоснабжения	У, С, П	сотрудники, природные явления	Д

3.2.3 Идентификация уязвимостей активов автоматизированной системы

Целью данного процесса - определение перечня уязвимостей актива и их оценка. Угроза ИБ может использовать множество уязвимостей актива или активов, в то же время уязвимость может быть использована некоторым множеством угроз ИБ.

Идентификация уязвимостей ИБ ас предприятия представляет собой определение слабостей в физической среде организации в каких-то

процедурах, уязвимости сотрудников, в управлении, в аппаратных и программных средствах, которые могут быть использованы источниками угроз, чтобы причинить ущерб активам системы, и, следовательно, деятельности ООО «Росток - мебель».

Уязвимости актуальные для системы представлены в таблице 13.

Таблица 13 – Перечень уязвимостей

Тип актива	Уязвимость	Описание
Аппаратные и программные средства	УЯ31	Недостаточное техническое обслуживание
	УЯ32	Отсутствие периодической замены оборудования
	УЯ33	Широко известные дефекты программных средств
	УЯ34	Неправильные параметры установки
	УЯ35	Отсутствие «выхода из системы» при покидании рабочего места
	УЯ36	Неконтролируемая загрузка и использование программных средств
	УЯ37	Плохое управление паролями
Сеть	УЯ38	Ненадежная сетевая архитектура
	УЯ39	Ненадежное управление сетью
Персонал	УЯ310	Неадекватные процедуры набора персонала
	УЯ311	Отсутствие осведомленности о безопасности
	УЯ312	Ненадлежащее использование программных и аппаратных средств
	УЯ313	Отсутствие механизмов мониторинга

Продолжение таблицы 13

Тип актива	Уязвимость	Описание
Место функционирования организации	УЯЗ14	Нестабильное электропитание
	УЯЗ15	Неадекватное или небрежное использование механизмов физического контроля доступа в здание, комнаты и офисы
	УЯЗ16	Отсутствие регулярных аудитов (проверок)

Уязвимости активов представлены в таблице 14.

Таблица 14 – Уязвимости активов

Актив	Уязвимость	Связанные уязвимости
Основные активы		
ИА1	Уяз2, 5, 12-13, 15	Уяз1-16
ИА2	Уяз2, 5, 12-13, 15	Уяз1-16
ИА3	Уяз2, 5, 12-13, 15	Уяз1-16
ИА4	Уяз2, 5, 12-13, 15	Уяз1-16
ИА5	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА6	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА7	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА8	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА9	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА10	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА11	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА12	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА13	Уяз2, 5, 7, 12-13, 15	Уяз1-16
ИА14	Уяз2, 5, 7, 12-13, 15	Уяз1-16
Вспомогательные активы		
ВА1	Уяз1-3, 11, 12, 14-26	Нет
ВА2	Уяз1-3, 11, 12, 14-26	Нет
ВА3	Уяз1-3, 11, 12, 14-26	Нет
ВА4	Уяз1-10, 11-16	Нет
ВА5	Уяз1-10, 11-16	Нет
ВА6	Уяз1-10, 11-16	Нет
ВА7	Уяз1-10, 11-16	Нет
ВА8	Уяз1-10, 11-16	Нет
ВА9	Уяз1-10, 11-16	Нет
ВА10	Уяз1-10, 11-16	Нет

Продолжение таблицы 14

Актив	Уязвимость	Связанные уязвимости
Основные активы		
BA11	Уяз1-10, 11-16	Нет
BA12	Уяз1-10, 11-16	Нет
BA13	Уяз1-10, 11-16	Нет

Идентификация последствий.

Цель процесса - идентификация последствий в результате потери целостности, доступности, конфиденциальности активов.

Последствия – результат события, оказывающее влияние на цели.

В качестве события рассматривается инцидент. Инцидент ИБ – это одно или серия нежелательных событий ИБ, которые имеют значительную вероятность компрометации бизнес-операций и угрожают ИБ.

В соответствии с ГОСТ Р ИСО/МЭК 27002-2012 [7] сценарий инцидента является описанием угрозы, использующей определенную уязвимость или набор уязвимостей актива во время инцидента ИБ.

Возможные последствия сценариев инцидентов приведены в таблице 15.

Таблица 15 – Возможные последствия сценариев инцидентов

№	Описание последствий
П1	Потеря времени на ремонт и рабочего времени для замены или восстановления актива
П2	Упущенная возможность, вследствие того, что финансовые ресурсы, необходимые для замены или восстановления актива, использовались бы где-то в другом месте
П3	Снижение безопасности сотрудников вследствие нарушения ИБ
П4	Финансовые затраты, связанные, со стоимостью восстановления потерянного актива
П5	Финансовые затраты на получение специфических навыков, необходимых для устранения неисправности
П6	Потеря репутации вследствие нарушения законодательных или нормативных обязательств

В таблице 16 представлен перечень возможных нежелательных событий в системе.

Таблица 16 – События информационной безопасности

Событие	Описание
C1	Выход из строя АРМ сотрудника с частичной или полной потерей, хранимой и обрабатываемой на нем информации
C2	Выход из строя сетевого оборудования
C3	Выход из строя программного обеспечения
C4	Нарушение конфиденциальности отчетной документации
C5	Нарушение целостности или доступности персональных данных, затруднение деятельности на период восстановления

3.3 Анализ риска информационной безопасности

3.3.1 Оценка последствий

Целью процесса оценки последствий является оценка влияния инцидентов ИБ на бизнес организации (оценка последствий) с учётом последствий нарушения ИБ.

Ввиду отсутствия защитных мер, тяжесть последствий реализации сценария инцидента равна максимальной стоимости среди активов, которые он затрагивает.

3.3.2 Оценка вероятности инцидента

Цель процесса – оценка вероятности сценариев инцидентов. Она проводится с целью выявления оценки возможных сценариев инцидента. Для оценки вероятностей инцидента необходимо использовать перечень сценариев инцидентов с их последствиями и оценками последствий.

Были учтены оценки возможности реализации угроз и оценки возможности использования уязвимостей.

Были введены следующие обозначения возможности реализации угроз и использования уязвимостей:

- низкая возможность;
- средняя возможность;
- высокая возможность,
- критическая возможность.

Вероятность инцидента была вычислена с помощью таблицы 17. Низкой вероятности инцидента поставлена в соответствии единица.

Таблица 17 – Таблица соответствия оценки вероятности инцидента возможности реализации угрозы и возможности использования уязвимости на предприятии ООО «Росток-мебель»

Возможность реализации угрозы	Низкая			Средняя			Высокая		
Возможность использования уязвимости	Н	С	В	Н	С	В	Н	С	В
Оценка вероятности инцидента	1	2	3	2	3	4	3	4	5

Результат оценки вероятности представлен в таблице 18.

Таблица 18 – Оценка вероятности инцидента

№	Возможность реализации угрозы	Возможность использования уязвимости	Вероятность инцидента
СИ1	1	2	2
СИ2	2	1	2
СИ3	2	1	2
СИ4	2	1	2
СИ5	2	2	3
СИ6	3	2	4
СИ7	2	2	3
СИ8	2	2	3
СИ9	3	2	4
СИ10	3	2	4
СИ11	1	1	1

3.3.3 Определение уровня риска

Для определения уровня риска был использован способ ранжирования угроз мерами риска, который связывает ценность активов с вероятностью возникновения угрозы. Ранжирование угроз мерами риска представлено в таблице 19.

Таблица 19 – Ранжирование угроз мерами риска

Идентификатор угрозы	Последствия (ценность актива)	Возможность возникновения угрозы	Мера риска	Ранжирование угроз
У1	5	1	5	9
У2	3	2	6	5

Продолжение таблицы 19

Идентификатор угрозы	Последствия (ценность актива)	Возможность возникновения угрозы	Мера риска	Ранжирование угроз
У3	3	2	6	6
У4	3	2	6	4
У5	4	3	12	2
У6	4	3	12	1
У7	3	3	9	3
У8	3	2	6	7
У9	3	2	6	8

После ранжирования угроз мерами риска, были определены приоритеты для различных угроз с разными последствиями и возможностью их возникновения.

В результате был получен перечень рисков с их описанием. Перечень рисков в порядке убывания их приоритета:

- потеря репутации вследствие нарушения законодательных или нормативных обязательств из-за нарушения конфиденциальности активов: «Информация о безработных гражданах», «Отчетная документация» путем реализации угрозы «Кража носителей информации или документов» с использованием уязвимостей: «Неадекватные процедуры набора персонала», «Отсутствие осведомленности о безопасности», «Ненадлежащее использование программных и аппаратных средств»;

- потеря времени на ремонт и рабочего времени для замены или восстановления актива, упущенная возможность, вследствие того, что финансовые ресурсы, необходимые для замены или восстановления актива, использовались бы где-то в другом месте и финансовые затраты, связанные, со стоимостью восстановления потерянного актива из-за нарушения конфиденциальности и доступности активов: «Заявление от безработных граждан», «Персональные данные в БД, бумажные заявления», «Персональные данные в БД», «Информация о безработных гражданах», «Заявки работодателей», «Данные о вакансиях», «Регистрационные записи в

БД о безработных гражданах и вакансиях», «Отчетная документация» и «Сетевое оборудование» путем реализации угрозы «Кража оборудования» с использованием уязвимостей: «Неадекватные процедуры набора персонала», «Неадекватное или небрежное использование механизмов физического контроля доступа в здание, комнаты и офисы»;

– потеря репутации вследствие нарушения законодательных или нормативных обязательств из-за нарушения конфиденциальности, доступности, целостности активов: «Заявление от безработных граждан», «Персональные данные в БД, бумажные заявления», «Персональные данные в БД», «Информация о безработных гражданах», «Заявки работодателей», «Данные о вакансиях», «Регистрационные записи в БД о безработных гражданах и вакансиях», «Отчетная документация» путем реализации угрозы «Несоблюдение требований по защите информации» с использованием уязвимостей: «Неверное распределение прав доступа», «Отсутствие «выхода из системы» при покидании рабочего места», «Плохое управление паролями», «Отсутствие осведомленности о безопасности», «Неадекватное или небрежное использование механизмов физического контроля доступа в здание, комнаты и офисы»;

– потеря времени на ремонт и рабочего времени для замены или восстановления актива, финансовые затраты, связанные со стоимостью восстановления потерянного актива, потеря репутации вследствие нарушения законодательных или нормативных обязательств из-за нарушения целостности активов: «Заявление от безработных граждан», «Персональные данные в БД, бумажные заявления», «Персональные данные в БД», «Информация о безработных гражданах», «Заявки работодателей», «Данные о вакансиях», «Регистрационные записи в БД о безработных гражданах и вакансиях», «Отчетная документация» путем реализации угрозы «Искажение информации» с использованием уязвимостей: «Отсутствие «выхода из системы» при покидании рабочего места», «Плохое управление паролями»;

– потеря времени на ремонт и рабочего времени для замены или восстановления актива, упущенная возможность, вследствие того, что финансовые ресурсы, необходимые для замены или восстановления актива, использовались бы где-то в другом месте, финансовые затраты, связанные, со стоимостью восстановления потерянного актива, потеря репутации вследствие нарушения законодательных или нормативных обязательств из-за нарушения доступности активов: «АРМ секретарей», «АРМ администраторов», «Сервер БД», «Сетевое оборудование», «Периферийное оборудование» путем реализации угрозы «Отказ оборудования» с использованием уязвимостей: «Недостаточное техническое обслуживание», «Отсутствие периодической замены оборудования», «Чувствительность к влажности, пыли, загрязнению», «Отсутствие контроля изменений конфигурации», «Неконтролируемое копирование», «Нестабильное электропитание»;

– потеря времени на ремонт и рабочего времени для замены или восстановления актива, упущенная возможность, вследствие того, что финансовые ресурсы, необходимые для замены или восстановления актива, использовались бы где-то в другом месте, финансовые затраты, связанные, со стоимостью восстановления потерянного актива из-за нарушения доступности актива – «Сетевое оборудование» путем реализации угрозы «Отказ сетевого оборудования» с использованием уязвимостей: «Недостаточное техническое обслуживание», «Отсутствие периодической замены оборудования», «Чувствительность к влажности, пыли, загрязнению», «Ненадежная сетевая архитектура», «Ненадежное управление сетью»;

– потеря времени на ремонт и рабочего времени для замены или восстановления актива, упущенная возможность, вследствие того, что финансовые ресурсы, необходимые для замены или восстановления актива, использовались бы где-то в другом месте из-за нарушения доступности и целостности активов: «Заявление от безработных граждан»,

«Персональные данные в БД, бумажные заявления», «Персональные данные в БД», «Информация о безработных гражданах», «Заявки работодателей», «Данные о вакансиях», «Регистрационные записи в БД о безработных гражданах и вакансиях», «Отчетная документация», «Прикладное ПО» путем реализации угрозы «Нарушение функционирования ПО» с использованием уязвимостей: «Широко известные дефекты программных средств», «Неконтролируемое копирование», «Неправильные параметры установки», «Неверное распределение прав доступа», «Неконтролируемая загрузка и использование программных средств»;

– упущенная возможность, вследствие того, что финансовые ресурсы, необходимые для замены или восстановления актива, использовались бы где-то в другом месте из-за нарушения доступности активов: «Заявление от безработных граждан», «Персональные данные в БД, бумажные заявления», «Персональные данные в БД», «Информация о безработных гражданах», «Заявки работодателей», «Данные о вакансиях», «Регистрационные записи в БД о безработных гражданах и вакансиях», «Отчетная документация», «АРМ секретарей», «АРМ администраторов», «Сервер БД», «Прикладное ПО», «Сетевое оборудование», «Периферийное оборудование» путем реализации угрозы «Нарушение энергоснабжения» с использованием уязвимости – «Нестабильное электропитание»;

– потеря времени на ремонт и рабочего времени для замены или восстановления актива, финансовые затраты, связанные со стоимостью восстановления потерянного актива из-за нарушения доступности и целостности активов: «АРМ секретарей», «АРМ администраторов» путем реализации угрозы «Пожар» с использованием уязвимостей: «Отсутствие периодической замены оборудования», «Чувствительность к влажности, пыли, загрязнению», «Неадекватные процедуры набора персонала», «Отсутствие осведомленности о безопасности», «Ненадлежащее использование программных и аппаратных средств», «Отсутствие механизмов мониторинга», «Нестабильное электропитание», «Неадекватное

или небрежное использование механизмов физического контроля доступа в здание, комнаты и офисы», «Отсутствие регулярных аудитов (проверок)».

3.4 Оценивание риска

Оценивание риска – процесс сравнения результатов анализа риска с критериями риска с целью определения является ли риск приемлемым.

Для оценивания рисков требуются перечни риска с установленными значениями уровней рисков, критерии оценивания и критерии принятия рисков. Оценивание риска основывается на результатах анализа риска и необходимо для принятия решений о будущих действиях

Для оценивания риска следует использовать следующую шкалу:

- низкий уровень риска: от 0 до 2;
- средний уровень риска: от 3 до 5;
- высокий уровень риска: от 6 до 8.

Приемлемым следует считать низкий уровень риска.

Результат оценивания рисков представлен в таблице 20.

Таблица 20 - Результат оценивания риска

Сценарий инцидента	Мера риска	Результат оценивания	Приемлемость
СИ1	3	Средний	Неприемлемый
СИ2	3	Средний	Неприемлемый
СИ3	3	Средний	Неприемлемый
СИ4	2	Низкий	Приемлемый
СИ5	2	Низкий	Приемлемый
СИ6	4	Средний	Неприемлемый
СИ7	4	Средний	Неприемлемый
СИ8	3	Средний	Неприемлемый
СИ9	4	Средний	Неприемлемый
СИ10	3	Средний	Неприемлемый
СИ11	2	Низкий	Приемлемый

4 Классификация информации в автоматизированной системе предприятия

В АС предприятия ООО «Росток - мебель» производится обработка конфиденциальной информации, в связи с этим должна производиться классификация циркулирующей информации в АС предприятия, это необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

Для проведения классификации необходимы следующие исходные данные:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- режим обработки данных в АС.

Информационным ресурсам предприятия ООО «Росток - мебель» присвоены уровни конфиденциальности: документы общего пользования (ДОП), информация ограниченного доступа (ИОД), персональные данные (ПДн), конфиденциальная информация (КИ) и секретная информация (СИ). Перечень информационных ресурсов с уровнями конфиденциальности представлен в таблице 21.

Таблица 21 – Перечень информационных ресурсов с уровнем конфиденциальности

Информационный ресурс	Уровень конфиденциальности
Нормативная и правовая документация	ДОП
Техническая документация	ИОД
Должностные инструкции	ИОД
Отчетность бухгалтерии	КИ
Отчетность отдела ИБ	КИ
Персональные данные	ПДн
Приказы и постановления директора	ДОП
Информация о продукции и услугах	ДОП
Договор об оказании услуг	СИ
Отчетная документация отдела маркетинга сбыта и информации	ИОД
Отчетность отдела работы с клиентами	ИОД
Отчетная документация планово-экономического отдела	ИОД
Отчетная документация отдела внешней комплектации и снабжения	ИОД

Для всех работников предприятия «Росток - мебель» установлены уровни доступа и полномочия. Уровни доступа разделены на: полный доступ к информации (ПДкИ) и ограниченный доступ к информации (ОГкИ). В зависимости от уровня доступа у каждого сотрудника свой список полномочий, который ограничивает его деятельность. Перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий представлены в таблице 22.

Таблица 22 - Перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий

Лица имеющее доступ к штатным средствам АС	Уровень доступа и список полномочий
Генеральный директор	ОГкИ: чтение, запись, изменение
Заместитель генерального директора	ОГкИ: чтение, запись, изменение
Системный администратор	ПДкИ: чтение, запись, изменение
Сотрудники отдела ИБ	ОГкИ: чтение, запись, изменение
Сотрудники отдела работы с клиентами	ОГкИ: чтение, запись, изменение

Продолжение таблицы 22

Лица имеющее доступ к штатным средствам АС	Уровень доступа и список полномочий
Сотрудники отдела маркетинга сбыта и информации	ОГКИ: чтение, запись, изменение
Сотрудники отдела кадров	ОГКИ: чтение, запись, изменение
Сотрудники отдела внешней комплектации и снабжения	ОГКИ: чтение, запись, изменение
Сотрудники отдела бухгалтерии	ОГКИ: чтение, запись, изменение

Режим обработки данных в АС предприятия ООО «Росток - мебель» зависит от деятельности конкретного отдела, например, в отделах «Отдел внешней комплектации и снабжения», «Отдел маркетинга сбыта и информации», «Планово-экономический отдел» и «Бухгалтерия» реализована пакетная обработка данных. По каждой задаче в соответствии с календарными сроками ее решения, например, обработка документов по составлению квартального баланса ООО «Росток - мебель», формируется пакет документов. При условии подготовки полного состава (пакета) документов эта задача ставится в очередь и при освобождении вычислительных ресурсов ЭВМ этот пакет запускается в обработку. Следующее задание может быть запущено только при условии окончания выполнения предшествующего задания.

С целью сокращения времени на обработку данных и рационализации вычислительных ресурсов в отделе «Отдел работы с клиентами» предприятия ООО «Росток - мебель» применяется мультипрограммный режим обработки данных, т.е. параллельная обработка данных по нескольким задачам пользователя. В отделе «Отдел ИБ» применяется диалоговый режим обработки данных в двух приемах формирования диалога: глобальный и локальный. При глобальном диалоге с помощью меню задается последовательность программ, характеризующих функциональные возможности программной системы. Локальный диалог формирует нужный алгоритм обработки по запросу пользователя.

Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

5 Анализ организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ООО «Росток - мебель»

5.1 Персональные данные, обрабатываемые в информационных системах персональных данных предприятия ООО «Росток - мебель»

Персональными данными является та информация, которая относится к прямому или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

В целях определения состава ПДн, обрабатываемых в информационных системах предприятия, классификации информационных систем ПДн и обеспечения необходимого уровня их защиты отделом информационной безопасности.

При разработке перечня ПДн, обрабатываемых в информационной системе предприятия ООО «Росток - мебель» определяются категории обрабатываемых ПДн следующих субъектов ПДн:

- клиенты предприятия/представители компаний-партнеров;
- сотрудники предприятия;
- кандидаты на соискание вакантной должности, профессии;
- посетители предприятия.

Перечень ПДн, обрабатываемых в ИСПДн предприятия актуализируется при необходимости, но не реже чем один раз в год. Необходимость корректировки перечня оценивается при модификации находящихся в эксплуатации информационных систем, вводе в эксплуатацию новых информационных систем, а также при изменении существующих процессов, в рамках которых обрабатываются ПДн.

Изменение в перечень ПДн вносятся решением совета по информационной безопасности предприятия.

Порядок взаимодействия должностных лиц с субъектами ПДн, в том числе реагирование на запросы субъектов ПДн или их законных

Сведения об обнаружении субъектов ПДн фиксируются в журнале учета обращений субъектов ПДн. Форма журнала представлена на рисунке 2.

ЖУРНАЛ УЧЕТА
обращений субъектов персональных данных в ООО «Росток - мебель»

Журнал завершен «__»_____20__г.
Должность
/ ФИО должностного лица /

№ П. п	Сведения о Запрашивающем лице	Краткое содержание обращения	Цель запроса	Отметка о предоставлении информации или об отказе в ее предоставлении	Дата передачи отказа в предоставлении информации	Подпись ответственного
1	2	3	4	5	6	7

Классификация локальных ИСПДн осуществляется комиссией по классификации ИСПДн предприятия. Состав для классификации локальных ИСПДн, а также порядок проведения классификации определяется локально нормативным актом предприятия. По результатам классификации оформляется акт в соответствии с регламентом проведения классификации ИСПДн.

49

5.2 Принципы обработки персональных данных на предприятии ООО «Росток - мебель»

Предприятие ООО «Росток - мебель» применяет все необходимые меры по выполнению требований законодательства, не обрабатывает ПДн в случаях, когда это не допускается законами Российской Федерации, не использует ПДн во вред субъектам.

Ограничение обработки ПДн достижением конкретных, заранее определенных и законных целей. Целями обработки ПДн на предприятии являются:

- в отношении сотрудников/ кандидаты на соискание вакантной должности, профессии – содействие в трудоустройстве, обучение и продвижении по службе, обеспечении личной безопасности работников, контроль качества выполняемой работы и обеспечение сохранности имущества предприятия;

- в отношении клиенты предприятия/представители компаний-партнеров – обеспечение возможности доступа на объекты предприятия в соответствии с установленными правилами пропускного режима, оказание предприятием коммерческих услуг.

Обработка только тех ПДн, которые отвечают заранее объявленным целям их обработки. Соответствие содержания и объема обрабатываемых ПДн заявленным целям обработки. Недопущение обработки ПДн несовместимой с целями сбора ПДн. Недопущение обработки избыточных ПДн по отношению к заявленным целям их обработки.

Недопущение объединения баз данных, содержащих ПДн, обработка которых осуществляется в целях, не совместимых между собой.

Обеспечение точности, достаточности и актуальности ПДн по отношению к целям обработки ПДн. Предприятие принимает все разумные меры по поддержке актуальности обрабатываемых ПДн, включая, но не ограничиваясь, реализацией каждого субъекта получать для ознакомления свои персональные данные (кроме случаев ограничения этого права

федеральными законами) и требовать от предприятия их уточнения, блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, неточными, незаконно полученными или не являются необходимыми для заявленных целей обработки.

Уничтожение, либо обезличивание ПДн по достижении заявленных целей их обработки или в случае утраты необходимости в достижении этих целей, при невозможности устранения предприятием допущенных нарушений ПДн, если иное не предусмотрено федеральными законами.

5.3 Условия обработки персональных данных на предприятии ООО «Росток - мебель»

Обработки персональных данных необходима для достижения целей, предусмотренных законодательством Российской Федерации об обязательных видах страхования, страховым законодательством, законодательством о государственной социальной помощи, трудовым законодательством, законодательством о пенсиях по государственному пенсионному обеспечению, о трудовых пенсиях, для осуществления и выполнения возложенных законодательством Российской Федерации на предприятие функций, полномочий и обязанностей.

Для исполнения договора, стороной которого, либо выгодоприобретателем или поручителем, по которому является субъект ПДн, а также для заключения договора по инициативе субъекта ПДн или договора, по которому субъект ПДн будет являться выгодоприобретателем или поручителем. Такими договорами являются:

- гражданско-правовые договора с сотрудником предприятия;
- договора об оказании коммерческих услуг клиентам предприятия.

В отношении кандидатов преддоговорной работой является работа по подбору персонала, в которой согласие субъекта на обработку подтверждается собственноручно заполненной и переданной предприятию анкетой соискателя должности/профессии с заполненным разделом,

подтверждающим согласие субъекта на обработку его ПДн. В отношении клиентов преддоговорной является деятельность с целью заключить в дальнейшем договор с клиентом или договор, выгодоприобретателем по которому является клиент.

Обработка ПДн необходима для осуществления прав и законных интересов предприятия или третьих лиц, установленных законодательством Российской Федерации или нормативно-правовыми актами органов управления связью либо для достижения общественно значимых целей при условии, что при этом не нарушаются права и свободы субъекта ПДн. К такой деятельности относится предоставление сведений в федеральные органы исполнительной власти и/или определенные ими организации, деятельность по совершенствованию оказываемых услуг, созданию новых услуг предприятия.

Обработка ПДн осуществляется в статистических или исследовательских целях при условии обязательного обезличивания ПДн.

Обработка ПДн осуществляется в целях противодействия легализации (отмыванию) доходов, полученных преступным путем и финансирования терроризма.

Доступ неограниченного круга лиц к ПДн предоставлен субъектом ПДн либо по его просьбе.

Предприятие не раскрывает третьим лицам и не распространяет ПДн без согласия субъекта ПДн, если иное не предусмотрено федеральным законом или нормативно-правовыми актами федеральных органов исполнительной власти.

Предприятие осуществляет трансграничную передачу ПДн только в следующих случаях:

- при наличии согласия в письменной форме субъекта ПДн на трансграничную передачу его ПДн;
- когда это предусмотрено международными договорами Российской Федерации;

— для исполнения договора, стороной которого является сотрудник или клиент, предусматривающего трансграничную передачу персональных данных.

Предприятие не принимает решений, порождающих юридические последствия в отношении субъекта ПДн или иным образом затрагивающих права и законные интересы субъектов, на основании исключительно автоматизированной обработки персональных данных. Данные, имеющие юридические последствия или затрагивающие права и законные интересы субъекта, перед их использованием подлежат проверке со стороны уполномоченных соответствующим образом подразделений предприятия.

5.4 Согласие субъекта на обработку персональных данных

Субъект ПДн принимает решение о предоставлении его ПДн предприятию и дает согласие на их обработку свободно, своей волей и в своем интересе. Согласие на обработку ПДн должно быть конкретным, информированным и сознательным и может предоставляться субъектом в любой, позволяющей подтвердить факт его получения, форме, если иное не установлено федеральным законом.

В случае получения согласия на обработку ПДн от представителя субъекта ПДн полномочия данного представителя на дачу согласия от имени субъекта ПДн проверяются предприятием.

ПДн сотрудников предприятия обрабатываются в соответствии с Положением о защите персональных данных работников ООО «Росток - мебель».

Специально выраженного согласия сотрудника на обработку его ПДн не требуется, т.к. обработка необходима для исполнения трудового договора, стороной которого является сотрудник-субъект ПДн, за исключением случаев, когда необходимо получение согласия сотрудника в письменной форме для конкретных случаев обработки ПДн. Такое согласие в письменной форме необходимо, но не исчерпывается следующими случаями:

- включение ПДн сотрудника в общедоступные источники ПДн;

- обработка специальных категорий ПДн, в том числе обработка сотрудниками предприятия, профессионально не занимающимися медицинской деятельностью и обязанными в соответствии с законодательством Российской Федерации сохранять врачебную тайну, сведений о состоянии здоровья сотрудника, не связанных с возможностью выполнения им трудовой функции;

- обработка биометрических ПДн сотрудника, в том числе его фотографических изображений, используемых для установления личности;

- трансграничная передача ПДн сотрудника на территории иностранных государств, не обеспечивающих адекватной защиты прав субъектов ПДн. Государствами, обеспечивающими адекватную защиту, являются государства-стороны Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн и государства, включенные в специальный перечень, утверждаемый Роскомнадзором;

- получение ПДн сотрудников у третьих лиц, в том числе с целью их проверки, а также в случаях, когда данные нельзя получить у самого сотрудника;

- сообщение ПДн сотрудника третьим лицам.

Согласие сотрудника в письменной форме на обработку ПДн может даваться не в виде отдельного документа, а закрепляться трудовым договором (дополнительным соглашением к нему) при условии включения в него сведений, установленных ч.4 ст.9 Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных». [2]

Согласие кандидата на соискание вакантной должности предприятия на обработку его ПДн требуется в случаях, предусмотренных Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных». [2]

Специально выраженного согласия клиента на обработку его ПДн не требуется, так как обработка ПДн необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем, по которому

является клиент-субъект ПДн, а также для заключения договора по инициативе клиента или договора, по которому клиент будет являться выгодоприобретателем.

Специально выраженного согласия посетителя на обработку его ПДн не требуется. Фактом получения согласия посетителя является добровольное предоставление в службу охраны предприятия документа, удостоверяющего личность, так как согласно режиму безопасности, установленному на объектах ООО «Росток - мебель» оформление пропусков и проход посетителей на территории предприятия, допускается только по предъявлению документа, удостоверяющего личность.

ПДн представителей контрагентов, содержащиеся в единых государственных реестрах юридических лиц и индивидуальных предпринимателей, являются открытыми и общедоступными, за исключением сведений о номере, о дате выдачи и об органе, выдавшем документ, удостоверяющий личность физического лица. Охраны их конфиденциальности и согласия субъектов на обработку не требуется. Во всех остальных случаях необходимо получение согласия субъектов ПДн, представляющих интересы контрагентов, при возникновении правоотношений с предприятием.

Обязанность предоставить доказательство получения согласия субъекта ПДн на обработку его ПДн или доказательство наличия оснований, указанных в Федеральном законе от 27.07.2006 № 152-ФЗ «О персональных данных», возлагается на ООО «Росток - мебель». [2]

Согласие на обработку ПДн может быть отозвано субъектом ПДн.

5.5 Доступ к персональным данным

5.5.1 Организация внутреннего доступа к персональным данным субъектов персональных данных

Сотрудники предприятия могут быть ознакомлены только с теми ПДн, которые необходимы им для выполнения своих служебных обязанностей.

Руководители структурных подразделений по управлению персоналом территориальных подразделений предприятия всех уровней ведут учет должностей и квалификационных характеристик работников, в служебные обязанности которых входит обработка ПДн.

В случае обнаружения нарушений установленных на предприятии правил предоставления ПДн, руководством предприятия может быть принято решение о приостановке предоставления ПДн до выявления и устранения причин нарушений.

5.5.2 Предоставление субъекту персональных данных доступа к своим персональным данным

Субъект ПДн имеет право на получение информации, касающейся обработки его ПДн, в том числе содержащей:

- подтверждение факта обработки ПДн предприятием;
- правовые основания и цели обработки ПДн;
- применяемые предприятием способы обработки ПДн;
- наименование и место нахождения предприятия, сведения о лицах (за исключением сотрудников предприятия), которые имеют доступ к ПДн или которым могут быть раскрыты ПДн на основании договора с предприятием (при его наличии) или на основании федерального закона;
- обрабатываемые ПДн, относящиеся к соответствующему субъекту ПДн, источник их получения;
- сроки обработки ПДн, в том числе сроки их хранения;
- информацию об осуществленной или о предполагаемой трансграничной передаче данных;
- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку ПДн по поручению оператора, если обработка поручена или будет поручена такому лицу;
- иные сведения, предусмотренные федеральными законами.

Сведения о наличии ПДн должны быть предоставлены субъекту ПДн предприятием в доступной форме, и в них не должны содержаться ПДн, относящиеся к другим субъектам ПДн.

Запрос субъекта об обработке его ПДн предприятием должен содержать:

- фамилию, имя и отчество субъекта ПДн;
- номер основного документа, удостоверяющего личность субъекта ПДн или его представителя (если запрос направлен представителем), сведения о дате выдачи указанного документа и выдавшем его органе;
- сведения, подтверждающие участие субъекта ПДн в отношениях с предприятием (номер, дата заключения договора, копия письма, направленного в адрес субъекта и т.д.), либо сведения, иным образом подтверждающие факт обработки ПДн предприятием;
- подпись субъекта ПДн или его представителя.

В случае, если обрабатываемые ПДн были предоставлены для ознакомления субъекту ПДн по его запросу, субъект ПДн вправе обратиться повторно к предприятию или направить повторный запрос в целях получения таких сведений и ознакомления со своими ПДн не ранее чем через тридцать дней после первоначального обращения или направления первоначального запроса, если более короткий срок не установлен федеральным законодательством или принятым в соответствии с ним нормативным правовым актом или договором, стороной которого либо выгодоприобретателем или поручителем по которому является субъект ПДн.

Повторный запрос должен содержать обоснование направления повторного запроса.

При отсутствии в запросе субъекта требуемых сведений, или несоблюдении сроков и условий направления запроса, предприятие вправе отказать субъекту в предоставлении запрашиваемых сведений.

Субъект ПДн вправе требовать от предприятия уточнения своих ПДн, их блокирования или уничтожения в случае, если ПДн являются неполными, устаревшими, недостоверными, незаконно полученными или не являются

необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав.

Если субъект ПДн считает, что предприятие осуществляет обработку его ПДн с нарушением требований федерального законодательства или иным образом нарушает его права и свободы, субъект ПДн вправе обжаловать действия или бездействие предприятия в уполномоченном органе по защите прав субъектов ПДн.

Субъект ПДн имеет право на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

5.6 Ответственность за нарушение норм, регулирующих обработку и обеспечение безопасности персональных данных

Сотрудники предприятия, виновные в нарушении требований действующего федерального законодательства Российской Федерации в области ПДн и требований положения, несут уголовную, административную, дисциплинарную и иную ответственность, предусмотренную законодательством Российской Федерации.

Юридические лица, нарушившие договорные обязательства перед предприятием по обеспечению конфиденциальности переданных (предоставленных) им ПДн, несут гражданско-правовую ответственность в соответствии с законодательством Российской Федерации.

5.7 Технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Росток - мебель»

5.7.1 Существующие технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Росток - мебель»

Программно-технические меры защиты информации - это совокупность аппаратных и программных средств и мероприятий по их использованию в интересах защиты конфиденциальности информации.

На предприятии осуществляется управление доступом путем деления информации по соответствующим должностям и полномочиям доступа к ней, т.е. спецификация и контроль действий пользователей над информационными ресурсами организации.

Программно-аппаратным средством защиты информации является SHDSL-модем с возможностью работать в режиме маршрутизатора для закрытия сети от проникновения извне.

SHDSL модем ZyXEL предназначен для создания корпоративной сети, в основе которой лежит скоростное двунаправленное соединение по медным проводам. Используется для объединения двух офисов по одной или по двум медным парам в режиме "точка-точка" с организацией симметричного скоростного полнодуплексного соединения. Модем имеет возможность работать в режиме моста или маршрутизатора. Встроена система обнаружения и предотвращения вторжений (Intrusion Detection System - IDS).

Для обеспечения защиты персональных компьютеров сотрудников предприятия от вредоносного программного обеспечения используется антивирусное программное обеспечение Kaspersky Internet Security 2015, установленное на все компьютеры. Kaspersky Internet Security - это программное решение для обеспечения оптимального уровня безопасности компьютера. Инновационная гибридная защита быстро устраняет вредоносные программы, спам и другие интернет-угрозы, экономя ресурсы компьютера за счет комбинации антивирусных и облачных технологий. Также администратор информационной безопасности имеет возможность непосредственного доступа к антивирусной защите всех компьютеров сотрудников предприятия, по средствам Kaspersky Security Center, единой консоль для управления решениями для защиты рабочих мест и управления всеми защитными продуктами.

В перечень свойств Kaspersky Security Center входит:

- гибкий контроль всех функций защиты рабочих мест;

- создание централизованных политик безопасности для различных платформ, включая Windows, Linux и Mac;
- управление системой предотвращения вторжений (HIPS) и сетевым экраном;
- настройка параметров безопасности для отдельных устройств, так и для групп;
- управление параметрами облачной защиты с использованием сети Kaspersky Security Network (KSN);
- мониторинг уязвимостей и управление установкой исправлений Kaspersky Security Center упрощает выявление и устранение уязвимостей в операционных системах и приложениях, позволяя быстрее устанавливать исправления;
- учет и управление IT-ресурсами. Все аппаратное и программное обеспечение в сети автоматически обнаруживается и заносится в реестры, что дает администратору полное представление обо всех ресурсах, которые нуждаются в защите и управлении;
- развертывание программного обеспечения (ПО) Автоматическое развертывание ПО, а также проверяемый удаленный доступ и устранение неполадок сокращают затраты времени и ресурсов на настройку новых рабочих станций и установку новых приложений;
- развертывание операционных систем (ОС) Kaspersky Security Center предоставляет централизованный контроль за созданием, хранением и копированием защищенных образов систем, чтобы оптимизировать и ускорить развертывание ОС. Поддерживается интерфейс UEFI;
- управление на уровне предприятия. Разграничение прав администраторов по ролям и поддержка популярных SIEM-систем помогают упростить управление сложными IT-средами.

Окно Kaspersky Security Center приведено на рисунке 3.

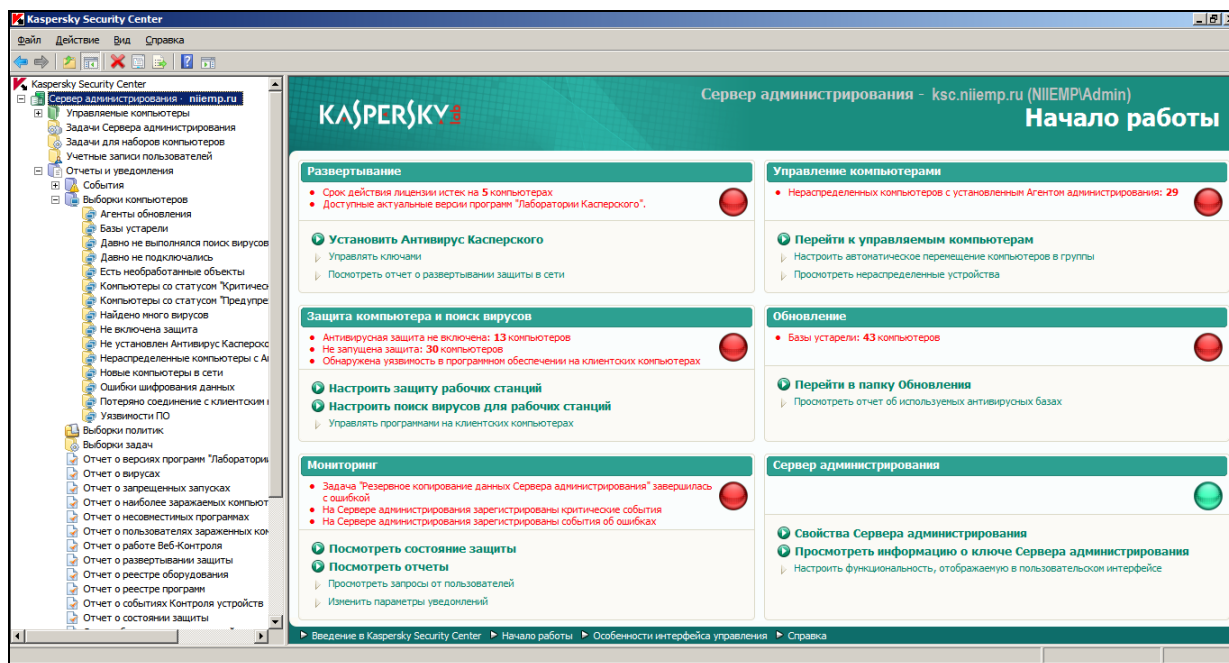


Рисунок 3 – Kaspersky Security Center

Kaspersky Security Center обеспечивает контроль всех параметров IT-безопасности, а также дает централизованный доступ к широкому спектру функций управления системами.[11]

5.7.2 Требуемые технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных ООО «Росток - мебель»

В число технических мер, связанных с обеспечением безопасности персональных данных, которые реализуются в рамках системы защиты персональных данных, учитывающей актуальные угрозы безопасности персональным данным и применяемые информационные технологии, требуется включить:

- идентификацию и аутентификацию объектов и субъектов доступа;
- возможность управления доступом субъектов к объектам доступа;
- возможность ограничения программных сред;
- регистрацию событий безопасности;
- антивирусную защиту;

- предотвращение (обнаружение) вторжений;
- анализ (контроль) степени защиты персональных данных;
- обеспечение целостности персональных данных и информационной системы;
- обеспечение доступа к персональным данным;
- защиту среду виртуализации;
- защиту технических средств;
- защита информационных систем, их средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурациями информационных систем и систем защиты персональных данных.

Меры, связанные с идентификацией и аутентификацией объектов и субъектов доступа, непременно связаны с присвоением объектам и субъектам уникальных признаков (идентификаторов), сравнение оных идентификаторов с перечнем идентификаторов присвоенных, а также проверку принадлежности объектам (субъектам) доступа предъявленных ими идентификаторов (подтверждения подлинности).

Меры, связанные с управлением доступом субъектов доступа к объектам доступа обязаны обеспечивать управление привилегиями и правами субъектов доступа, разграничение их доступа к объектам доступа, основанное на совокупности введённых в информационных системах правил разграничения доступа, а кроме того, обеспечение контроля над соблюдением данных правил.

Меры, связанные с ограничением программных сред, должны гарантировать запуск и (или) установку только того программного обеспечения, которое разрешено к использованию в информационной

системе; или же исключать возможности запуска и (или) установки программного обеспечения, которое запрещено к использованию в информационной системе.

Меры, которые связаны с регистрацией событий безопасности, сводятся к сбору, записи, хранению и защите информации о событиях безопасности в информационной системе, а также возможности просмотреть и проанализировать информацию о данных событиях и реакцию на них.

Меры, которые связаны с антивирусной защитой, позволяют обнаруживать в информационных системах компьютерные программы либо иную компьютерную информацию, которая предназначена, чтобы несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовывать средства защиты информации. Также меры, связанные с антивирусной защитой, должны реагировать на обнаружение данных программ или иных единиц информации.

Меры, которые связаны с обнаружением (предотвращением) вторжений, должны гарантировать, что действия, которые происходят в информационных системах и направлены на несанкционированный доступ к информации, будут обнаружены и пресечены.

Меры, которые связаны с контролем (анализом) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

Меры, которые связаны с обеспечением целостности информационных систем и персональных данных должны гарантировать, что факты несанкционированных нарушений целостности информационных систем будут обнаружены, а все данные, повреждённые в результате подобных несанкционированных вторжений, будут восстановлены.

Меры, которые связаны с обеспечением доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

Меры, которые связаны с защитой среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре.

Меры, которые связаны с защитой технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы.

Меры, которые связаны с защитой информационных систем, их систем связи, средств, и систем передачи данных, должны гарантировать защищённость персональных данных во время взаимодействия информационных систем или ее отдельных сегментов с прочими информационными системами, а также информационно-телекоммуникационными сетями, используя архитектуру информационных систем и проектные решения, направленные на то, чтобы обеспечить безопасность персональных данных.

Меры, которые связаны с выявлением инцидентов и реагированием на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

Меры, которые связаны с управлением конфигурацией информационных систем и систем защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

- определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных;
- адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы;
- уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу;
- дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных.

По итогам анализа организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ООО «Росток - мебель» можно сделать вывод, что на предприятии ООО «Росток - мебель» существует перечень документов (организационные меры), регламентирующих обеспечение безопасности ПДн при их обработке в ИСПДн ООО «Росток - мебель», также присутствуют технические меры по обеспечению безопасности ПДн, а именно:

- SHDSL-модем, имеющий возможность работать в режиме маршрутизатора, чтобы закрывать сеть от вторжений извне;
- для обеспечения защиты персональных компьютеров сотрудников предприятия от вредоносного программного обеспечения применяются антивирусные программы Kaspersky Internet Security 2015 и Kaspersky Security Center;

— существует единая консоль, позволяющая управлять решениями для защиты рабочих мест и всей совокупностью защитных продуктов.

Из этого можно сделать вывод, что для повышения уровня защиты ПДн в ООО «Росток - мебель» необходимо включить дополнительные средства защиты информации.

6 Анализ материалов организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации

6.1 Концепция информационной безопасности ООО «Росток - мебель»

Основным документом, регламентирующим информационную безопасность на предприятии ООО «Росток - мебель» является Концепция информационной безопасности ООО «Росток - мебель» (далее - Концепция) устанавливает цели, задачи и принципы деятельности по обеспечению информационной безопасности предприятия, которыми руководствуется предприятие в своей деятельности, а также определяет систему взглядов на проблему защиты информации в ООО «Росток - мебель» и принципов достижения адекватного уровня безопасности.

Концепция определяет основные правовые, организационные и технические положения внутренней политики предприятия в области безопасности информационных технологий и защиты информации.

Целью принятия Концепции является:

- определение общих, базовых принципов организации и построения системы информационной безопасности предприятия;
- определение приоритетов развития предприятия в области обеспечения информационной безопасности;
- определение и реализации единой технической политики предприятия при построении системы информационной безопасности;
- формирование у сотрудников предприятия единого представления о ценности корпоративной информации, а также значимости деятельности, затрагивающей процессы обеспечения информационной безопасности.

Основные задачи, решаемые Концепцией:

- определение основных угроз информационной безопасности предприятия;
- определение критичных информационных активов (объектов защиты) предприятия;

- совершенствование нормативной базы предприятия в области обеспечения информационной безопасности;
- создание правовой и организационной основы для разработки процедур, предотвращающих или адекватно реагирующих на нарушение режима защиты информации.

Концепция разработана в соответствии с законодательством Российской Федерации на основе лучших отечественных и зарубежных практик, вошедших в национальные и международные стандарты.

Все локальные нормативные документы предприятия, а также планируемые и проводимые мероприятия, затрагивающие вопросы обеспечения информационной безопасности, разрабатываются в соответствии с Концепцией.

Концепция не затрагивает деятельность предприятия по обеспечению безопасности информации, содержащей сведения, составляющие в соответствии с законодательством Российской Федерации государственную тайну.

В Концепции определены основные меры по обеспечению информационной безопасности на предприятии. Детальные рекомендации по обеспечению защиты информации ограниченного доступа приведены в рамках конкретных технических проектов по защите соответствующих видов информации.

Изменения в концепцию вносятся решением куратора информационной безопасности по представлению совета по информационной безопасности предприятия.

Концепция не содержит подробного анализа рисков для бизнеса предприятия, эта тема рассмотрена в рамках отдельного проекта по обеспечению непрерывности бизнеса, в методологию которого заложены подходы, определенные в рамках стандартов «Управление непрерывностью бизнеса», требования ООО «Росток - мебель», учтены требования регулирующих органов в части сроков предоставления регламентированной

отчетности и обязательные сроки оказания услуг, определенных правилами оказания услуг коммерческой деятельности.

6.2 Регламент информационной безопасности ООО «Росток - мебель»

Регламент информационной безопасности ООО «Росток - мебель» (далее - Регламент) определяет организацию деятельности, направленной на практическую реализацию положений Концепции информационной безопасности ООО «Росток - мебель» (далее - Предприятие), обязанности и полномочия органов управления и сотрудников, участвующих в этом процессе, а также порядок взаимодействия между ними в процессе практической деятельности по реализации положений Концепции.

Целями Регламента информационной безопасности:

- приведение процессов построения и управления системой информационной безопасности в соответствие с требованиями российского законодательства, лучшим отечественным и международным практикам, сложившейся системе корпоративного управления Предприятия, реальным потребностям, организационно-штатной структуре и финансовым возможностям;
- создание условий для оперативного, неформального, и, в необходимых случаях, документируемого взаимодействия участников процесса обеспечения информационной безопасности всех уровней Предприятия, координации деятельности органов и ответственных лиц при обеспечении информационной безопасности;
- обеспечение участия в процессе всех заинтересованных подразделений и должностных лиц Предприятия;
- сочетание коллегиальности принятия наиболее важных решений в области информационной безопасности и персональной ответственности конкретных лиц за решение вопросов в ходе операционной деятельности, оперативное реагирование на инциденты информационной безопасности;
- определение порядка осуществления мониторинга состояния безопасности и управления инцидентами информационной безопасности.

Положения Регламента не распространяются на деятельность Предприятия, связанную с защитой информации, составляющей государственную тайну.

Изменения в настоящий Регламент вносятся после их утверждения генеральным директором Предприятия ООО «Росток - мебель» по представлению Совета по информационной безопасности.

6.3 Корпоративная и частные политики информационной безопасности ООО «Росток - мебель»

Также на предприятии ООО «Росток - мебель» существует Корпоративная политика. Корпоративная политика – это совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Корпоративная политика описывает:

- цели информационной безопасности;
- структуру корпоративного управления информационной безопасностью;
- способы управления рисками информационной безопасности;
- принципы обеспечения поддержки и проверки информационной безопасности;
- принципы по обеспечению осведомленности и обучению информационной безопасности организации;
- обстоятельства, при которых корпоративная политика информационной безопасности должна быть пересмотрена или скорректирована.

Для детализации требований корпоративной политики информационной безопасности в рамках определенной области на предприятии существуют частные политики информационной безопасности автоматизированной системы.

Частные политики содержат:

- цели и задачи обеспечения информационной безопасности;
- область действия, определение объектов защиты, уязвимостей, угроз;
- описание рисков информационной безопасности;
- требования информационной безопасности;
- технические средства и организационные меры по обеспечению информационной безопасности;
- обязанности по обеспечению информационной безопасности;
- контроль за реализацией политики;
- пересмотр политики.

Таким образом, на предприятии ООО «Росток - мебель» существуют документы в области информационной безопасности, которые регламентируют деятельность как предприятия в целом, так и отдельных подразделений. Главным документом является Концепция информационной безопасности предприятия ООО «Росток - мебель». Регламент информационной безопасности ООО «Росток - мебель» определяет организацию деятельности, направленной на практическую реализацию положений Концепции информационной безопасности ООО «Росток - мебель». Корпоративная политика, а также частные политики информационной безопасности для детализации требований корпоративной политики информационной.

7 Методика построения корпоративной системы защиты информации ООО «Росток - мебель»

7.1 Модель построения корпоративной системы защиты информации ООО «Росток - мебель»

Согласно ст. 20 Федерального закона “Об информации, информатизации и защите информации” [1] цели защиты информации определяются, как:

- предотвращение утечек, хищений, утрат, искажений, подделок информации;
- предотвращение несанкционированных действий, связанных с уничтожением, модификацией, искажением, копированием, блокированием информации;
- предотвращением иных форм незаконных вмешательств в информационные ресурсы и информационные системы.

Главную цель любых систем информационной безопасности можно видеть в том, чтобы обеспечить устойчивое функционирование объектов: предотвратить угрозы его безопасности, защитить законные интересы владельцев информации от противоправных посягательств, включая уголовно наказуемые деяния в рассматриваемой области отношений, которые предусмотрены УК Российской Федерации, обеспечить нормальную производственную деятельность всех подразделений объектов. Другую задачу можно охарактеризовать, как повышение качества предоставляемых услуг и гарантий безопасности имущественным правам и интересам клиентов.

Для этого необходимо:

- отнесение информации к категории ограниченного доступа (служебная тайна);
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению

ущерба (будь то финансовый, материальный и моральный), нарушению их развития и нормального функционирования;

- создание условий работы с минимально возможным риском для безопасности информационным ресурсам и риском нанесения разных видов ущерба;

- создание механизма и условий оперативного реагирования на возникающие угрозы информационной безопасности и реагирования на проявления негативных тенденций в работе, действенное пресечение посягательств на ресурсы – используя правовые, организационные и технические меры и средства, позволяющие обеспечить безопасность;

- создание условий, чтобы максимально возможным образом возместить и локализовать ущерб, наносимый неправомерными действиями юридических и физических лиц, таким образом, ослабив возможные негативные влияния последствий в нарушении информационной безопасности.

Выполняя работы, можно воспользоваться моделью построения корпоративных систем защиты информации, изображённой на рисунке 4. В основе данной модели лежит адаптация Общих Критериев [9] и проведение анализа рисков [10]. Данная модель отвечает:

- специальным нормативным документам, связанным с обеспечением информационной безопасности, принятым в РФ;

- международному стандарту ISO/IEC 15408 “Информационная технология – методы защиты – критерии оценки информационной безопасности”; [9]

- стандарту ISO/IEC 17799 “Управление информационной безопасностью”; [10]

- принимает во внимание тенденции развития российской нормативной базы (включая акты Гостехкомиссии РФ), относящейся к защите информации.



Рисунок 4 - Модель построения корпоративной системы защиты информации

ООО «Росток - мебель»

Представленная модель построения корпоративной системы защиты информации ООО «Росток - мебель» является совокупностью объективных внутренних и внешних факторов и их влияния на состояние информационной безопасности на объектах, а также на сохранность информационных или материальных ресурсов.

Принимается во внимание следующий набор факторов:

- угроз информационной безопасности, характеризующихся вероятностью реализации и вероятностью возникновения;
- уязвимостей системы контрмер (система информационной безопасности) или информационной системы, влияющих на вероятность реализации угроз;

– риск является фактором, отражающим возможный ущерб организации, если будет реализована угроза информационной безопасности: утечка информации и ее неправомерное использование (риск, в общем виде, отражает вероятные финансовые потери – косвенные или прямые).

7.2 Методика построения корпоративной системы защиты информации ООО «Росток - мебель»

Чтобы построить сбалансированную систему информационной безопасности, необходимо сначала проанализировать риски в области информационной безопасности. Затем на основе заданных критериев определяется оптимальный для организации уровень риска. Система информационной безопасности (контрмер) должна быть построена таким образом, чтобы был достигнут заданный уровень риска.

В ходе построения методики должны быть учтены взаимосвязи ресурсов. В частности, выход из строя некоего оборудования способен привести к потере данных или поломке иного критически важного элемента системы. Данные взаимосвязи являются определяющими с точки зрения ИБ для основы методики организации.

Методика строится следующим образом, определяется ценность выделенных ресурсов определяется их ценность, притом, с нескольких точек зрения (ассоциированные с ними возможные финансовые потери, ущерб репутации организации, дезорганизация ее работы, нематериальный ущерб от разглашения конфиденциальных данных и т.д.). После этого составляется описание взаимосвязей ресурсов, проводится определение угроз безопасности и оценка вероятности их проявления.

Основываясь на построенной методике, обоснованно выбирают систему контрмер, которые могли бы снизить риски до допустимого уровня и при этом, обладают наибольшей ценовой эффективностью. Часть системы контрмер будет состоять из рекомендаций по проведению проверок эффективности систем защиты на регулярной основе.

7.3 Проведение оценки технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений

Чтобы выполнить возникающие повышенные требования к ИБ, необходимо проведение соответствующих мероприятий на каждом этапе жизненного цикла информационной технологии. Данные мероприятия планируются, после того, как проведён анализ рисков и выбор контрмер. Обязательная составная часть данных планов состоит в периодической проверке соответствия существующего режима ИБ политикам безопасности, сертификации информационных систем (технологий) на соответствие требованиям определенных стандартов безопасности.

После завершения работы определяются меры гарантии безопасности информационных сред. В основе данной меры лежит оценка, насколько заслуживает доверия информационная среда объекта. Указанный подход предполагает, что применение больших усилий при проведении оценки безопасности влечёт за собой большую гарантию.

Список требований, предъявляемых к системам информационной безопасности, эскизному проекту, плану защиты (далее – техническая документация, ТД) включает комплекс требований безопасности информационных сред объекта. Данные требования могут содержать ссылки на соответствующие профили защиты, а также включать явно сформулированные требования.

В общем виде, разработка ТД состоит из:

- уточнения функций защиты;
- выбора архитектурных принципов построения СИБ;
- разработки логической структуры СИБ (четкого описания интерфейсов);
- уточнения требований функций обеспечения гарантоспособности СИБ;

- разработки методик и программ испытаний на соответствие их ранее сформулированным требованиям.

При оценке достигаемой защищенности, оценивают меру гарантии безопасности информационных сред. Меру гарантии основывают на оценке того, насколько после выполнения рекомендованных мероприятий заслуживает доверия информационная среда объекта. Согласно базовым положениям данной методики, предполагается, что степень гарантии зависит от того, насколько были эффективны усилия во время проведения оценки безопасности. Для роста количества усилий оценки предполагается:

- существенное число элементов информационных сред объекта, которые участвуют в оценивании;
- расширение номенклатуры типов проектов и описаний деталей выполнения в ходе проектирования систем, обеспечивающих безопасность;
- строгость, которая состоит в использовании большего числа методов и инструментов поиска, которые направлены на обнаружение не столь очевидных уязвимостей или на снижение вероятности их проявления.

Следовательно, данная методика позволяет оценивать или переоценивать уровень современного состояния защищенности информационных активов ООО «Росток - мебель», и кроме того, разработать рекомендации, связанные с обеспечением (повышением) информационной безопасности компании. В том числе, применение данных рекомендаций может позволить уменьшить потенциальные потери предприятия через повышение устойчивости работы корпоративной сети, создать политику и концепцию информационной безопасности ООО «Росток - мебель». Кроме того, указанная методика даёт возможность предложить планы защиты конфиденциальной информации данного предприятия, которая передаётся по открытым каналам связи, защиту информации компании от умышленных искажений (разрушений), несанкционированного доступа к информации, ее использования или копирования.

ЗАКЛЮЧЕНИЕ

В ходе выполнения работ были изучены подходы, способы и практики, применяемые для построения комплексной системы защиты информации на промышленных предприятиях.

Был проведён анализ существующих методов и средств, применяемых для контроля и защиты информации на предприятии ООО «Росток - мебель», были разработаны предложения по их совершенствованию и повышению их эффективности.

После этого были определены угрозы безопасности информации на предприятии ООО «Росток - мебель». Затем был произведен анализ организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных в ООО «Росток - мебель».

Далее были рассмотрены материалы организаций и подразделений ведомства с целью подготовки принятия решений по обеспечению защиты информации.

В результате проведенной работы была разработана методика построения корпоративной системы защиты информации ООО «Росток - мебель». Были проведены оценочные действия технико-экономического уровня и эффективности предлагаемых и реализуемых организационно-технических решений. Таким образом, все пункты технического задания выполнены полностью.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ФЗ «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана
2. ФЗ «О персональных данных» № 152-ФЗ от 27.07.2006 [Электронный ресурс]. Режим доступа: <http://docs.pravo.ru>, свободный. – Загл. с экрана.
3. Государственный стандарт № ГОСТ Р 51275-99 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию» [Электронный ресурс]. Режим доступа: <http://www.altell.ru/legislation/standards/51275-2006.pdf>, свободный. – Загл. с экрана.
4. Государственный стандарт № ГОСТ Р ИСО/МЭК 27001-2006 «Информационная технология. Методы и средства обеспечения безопасности. Система менеджмента информационной безопасности» [Электронный ресурс]. Режим доступа: <http://vsegost.com/Catalog/57/5736.shtml>, свободный. – Загл. с экрана.
5. Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы РФ». Аудит информационной безопасности» СТО БР ИББС-1.1-2007 [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_70433/, свободный. – Загл. с экрана.
6. Государственный стандарт № ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» [Электронный ресурс]. Режим доступа: <http://docs.pravo.ru>, свободный. – Загл. с экрана.
7. Государственный стандарт № ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения

безопасности. Свод норм и правил менеджмента информационной безопасности» [Электронный ресурс] Режим доступа: <http://www.internet-law.ru/gosts/gost/54705>, свободный. – Загл. с экрана.

8. Приказ ФСТЭК, Минюста России № 55/86/20, 11462 от 13.02.2008 «Об утверждении порядка проведения классификации информационных систем персональных данных» [Электронный ресурс]. Режим доступа: <http://docs.pravo.ru>, свободный. – Загл. с экрана.

9. Национальный стандарт РФ № ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. [Электронный ресурс]. Режим доступа: <http://docs.cntd.ru/document/gost-r-iso-mek-15408-1-2008>, свободный. – Загл. с экрана.

10. Национальный стандарт РФ № ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. [Электронный ресурс]. Режим доступа: <http://docs.cntd.ru/document/gost-r-iso-mek-17799-2005>, свободный. – Загл. с экрана.

11. Kaspersky Security Center [электронный ресурс]. – Режим доступа: <http://www.kaspersky.ru/security-center>, свободный. – Загл. с экрана.

ПРИЛОЖЕНИЕ А

(обязательное)

Структура участка локальной вычислительной сети бухгалтерии

Структура участка локальной вычислительной сети бухгалтерии

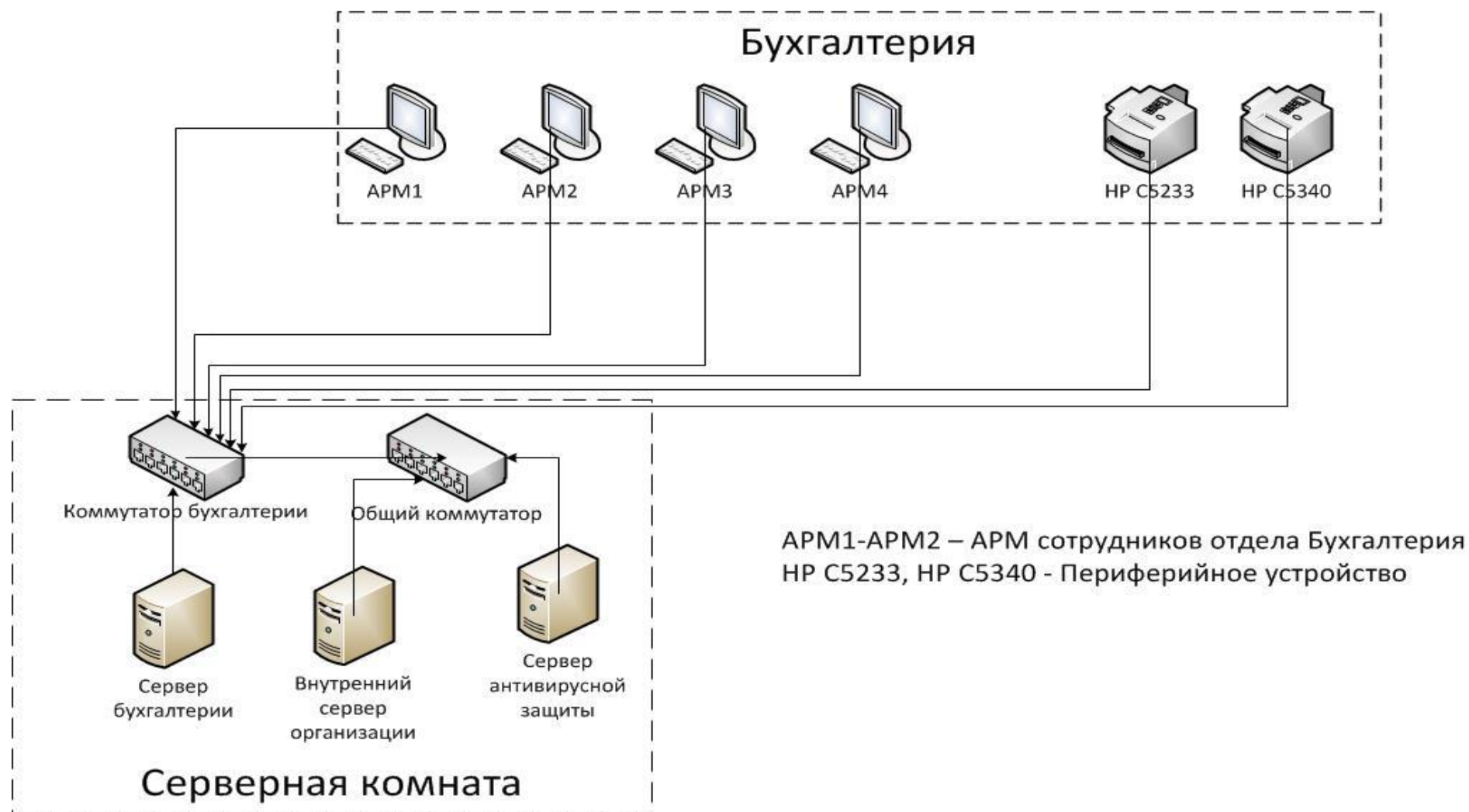


Рисунок А.1

ПРИЛОЖЕНИЕ Б

(обязательное)

Структура локальной вычислительной сети предприятия ООО «Росток
- мебель»

Структура локальной вычислительной сети предприятия ООО «Росток - мебель»

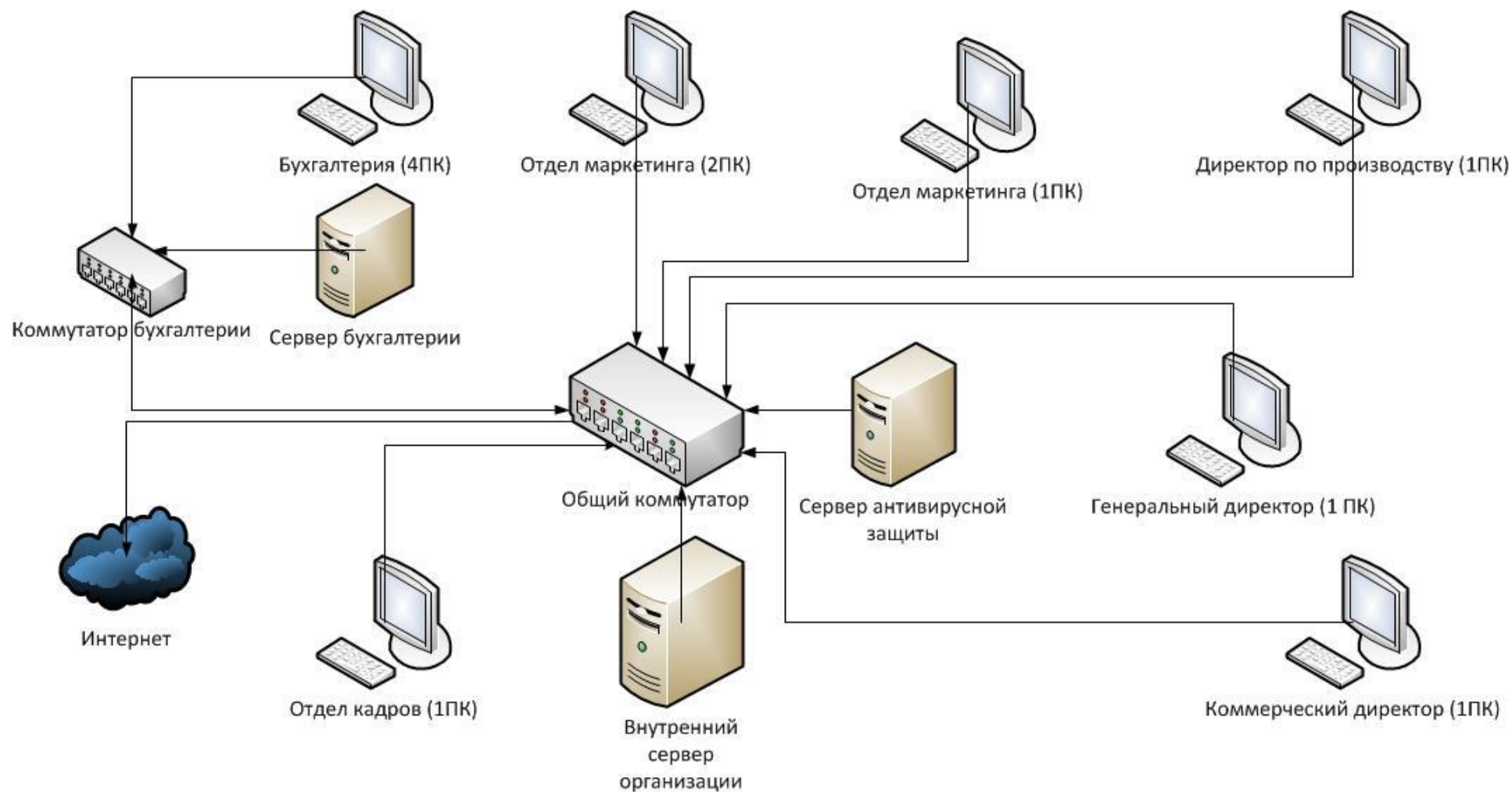


Рисунок Б.1

ПРИЛОЖЕНИЕ В

(обязательное)

Организационная структура предприятия ООО «Росток - мебель»

Организационная структура предприятия ООО «Росток - мебель»

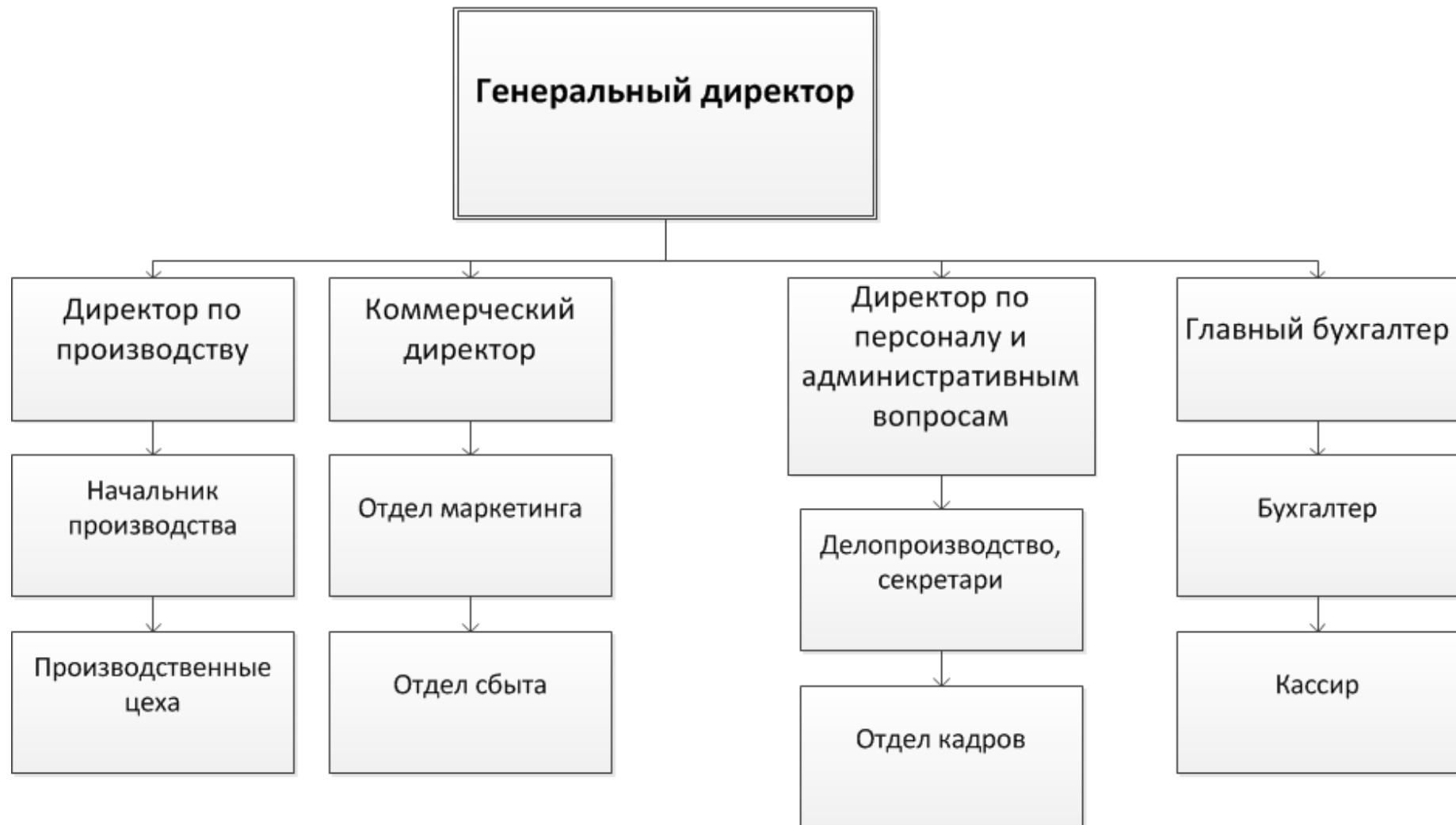


Рисунок В.1

