Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем
Направление подготовки 09.03.02 – Информационные системы и технологии
Направленность (профиль) образовательной программы: Безопасность информационных систем

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____2017 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Анализ и разработка рекомендаций по обеспечению информационной безопасности обособленного подразделения АО «Прииск Соловьевский»

Исполнитель студент группы 355-об	_____ (подпись, дата)	А.С. Нечипоренко
Руководитель доцент, канд.техн.наук	_____ (подпись, дата)	А.В. Бушманов
Консульт. по разд. безопасность и экологичность доцент, канд.техн.наук	_____ (подпись, дата)	А.Б. Булгаков
Нормоконтроль инженер кафедры	_____ (подпись, дата)	В.В. Романико

Благовещенск 2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)

Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____А.В.Бушманов
«_____»_____2017 г.

З А Д А Н И Е

К бакалаврской работе студента Нечипоренко Анну Сергеевну.

1. Тема бакалаврской работы: на тему: Анализ и разработка рекомендаций по обеспечению информационной безопасности обособленного подразделения АО «Прииск Соловьевский»

(утверждено приказом от 25.04.2017 № 929-уч)

2. Срок сдачи студентом законченной работы 20.06.2017 г.

3. Исходные данные к бакалаврской работе: отчет по преддипломной практике.

4. Содержание бакалаврской работы: анализ деятельности предприятия, анализ системы информационной безопасности, разработка политики безопасности, рассмотрение аспектов безопасности жизнедеятельности.

5. Перечень материалов приложения: организационная линейная структура, диаграммы, политика безопасности, техническое задание.

6. Консультант по бакалаврской работе консультант по безопасности и экологичности доцент, канд. техн. наук Булгаков А.Б.

7. Дата выдачи задания 09.05.2017 г.

Руководитель бакалаврской работы Бушманов Александр Вениаминович, доцент, канд. техн. наук.

Задание принял к исполнению (дата):_____А.С. Нечипоренко

РЕФЕРАТ

Бакалаврская работа содержит 68 с., 12 рисунков, 13 таблиц, 4 приложения, 18 источников.

ПОЛИТИКА БЕЗОПАСНОСТИ, РАЗРАБОТКА, СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РИСК, АНАЛИЗ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

Для данной бакалаврской работы объектом исследования была выбрана деятельность обособленного подразделения предприятия АО «Прииск Соловьевский» в г. Благовещенске.

Целью работы является разработка политики информационной безопасности.

Работа выполнялась последовательно в соответствие со следующими этапами: анализ деятельности предприятия, анализ системы информационной безопасности, разработка рекомендаций по обеспечению информационной безопасности, их экономическая обоснованность, разработка политики безопасности, а также исследование аспектов безопасности жизнедеятельности.

Разработанная политика информационной безопасности является высокоуровневым документом, который представляет собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности предприятия.

Политика безопасности разработана для всех работников, включая руководство обособленного подразделения АО «Прииск Соловьвский».

СОДЕРЖАНИЕ

НОРМАТИВНЫЕ ССЫЛКИ

Настоящая бакалаврская работа написала на основе следующих нормативных документов:

ГОСТ 2.104-68 ЕСКД Основные надписи

ГОСТ 2.105-95 ЕСКД Общие требования к текстовым документам

ГОСТ 2.106-96 ЕСКД Текстовые документы

ГОСТ 2.111-68 ЕСКД Нормоконтроль

ГОСТ 2.306-68 ЕСКД Обозначение графических материалов, правил нанесения их на чертежах

ГОСТ 2.316-68 ЕСКД Правила нанесения на чертежах надписей, технических требований и таблиц

ГОСТ 2.721-74 ЕСКД Обозначения условно-графические в схемах. Обозначения общего применения

ГОСТ 3.1105-84 ЕСКД Правила оформления документов общего назначения

ГОСТ 3.1130-93 ЕСКД Основные требования к формам и бланкам документов

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

ИС – информационная система;

БД – база данных;

ИБ – информационная безопасность;

БЖД – безопасность жизнедеятельности;

ВКР – выпускная квалификационная работа;

ПБ – политика безопасности;

НСД – несанкционированный доступ;

ОС – операционная система;

ПК – персональный компьютер;

ПО – программное обеспечение;

РД – руководящий документ;

РФ – Российская Федерация;

СВТ – средство вычислительной техники;

СУБД – система управления базами данных;

ТЗ – техническое задание;

МЭ – межсетевой экран;

АО – акционерное общество;

ОМТС – отдел материально технического снабжения;

ФЗ – федеральный закон;

ЛВС – локально-вычислительная сеть;

ССВ – совокупная стоимость владения.

ВВЕДЕНИЕ

Проблема обеспечения информационной безопасности с быстрым развитием технологий становится все более актуальной. Несмотря на несомненные преимущества информационного прогресса, это повлекло за собой ряд весьма специфичных проблем. Одной из них стала необходимость обеспечения эффективной защиты информации.

Деятельность любой организации в современном мире каждый день связана с различными рода рисками. Число попыток вторжений как на частные, так и на государственные организации постоянно растет. Целостность, достоверность и доступность информации в наши дни являются составными и важнейшими частями успеха любой организации.

Обеспечение вышеперечисленных аспектов информационной безопасности могут быть успешно решены с помощью создания и внедрения политики безопасности предприятия.

Политика безопасности представляет собой совокупность документированных административных решений, направленных на обеспечение безопасности информационных ресурсов.

Предприятия становятся все более заинтересованными в разработке политики безопасности, что объясняется необходимостью формирования основ планирования информационной безопасности и управления ею на современном этапе.

Соответственно, тема данной выпускной квалификационной работы «Анализ и разработка рекомендаций по обеспечению информационной безопасности для обособленного подразделения АО «Прииск Соловьевский»».

Итогом работы является разработанная политика информационной безопасности для обособленного подразделения предприятия АО «Прииск Соловьевский».

В работе были сформулированы следующие задачи:

– провести анализ предметной области, а именно описать деятельность предприятия, его организационную структуру, рассмотреть информационные потоки, описать аппаратно-техническое и программное обеспечение, выделить объект и предмет защиты;

– провести анализ системы информационной безопасности предприятия: идентифицировать и оценить активы, выявить уязвимости и угрозы ИБ, в соответствии с ними составить модель нарушителя, описать имеющиеся методы и средства защиты информации на предприятии, провести оценку рисков;

– исходя из анализа предметной области и системы ИБ, разработать многоуровневую политику безопасности предприятия;

– описать основы безопасности жизнедеятельности предприятия.

Теоретическая значимость работы состоит в создании политики безопасности предприятия – документа, включающего в себя принципы и правила, определяющие и ограничивающие виды деятельности объектов и участников, направленные на защиту информационных ресурсов.

Практическая значимость работы определяется тем, что ее результаты позволяют повысить степень защиты информации на предприятии путем внедрения политики безопасности.

Новизна бакалаврской работы заключается в первичной разработке политики информационной безопасности конкретно для данного обособленного подразделения предприятия.

1 АНАЛИЗ ПРЕДМЕТНОЙ ОБЛАСТИ

1.1 Описание предприятия и его организационной структуры

Акционерное общество «Прииск Соловьёвский» – золотодобывающее предприятие, занимающее первое место по уровню добычи россыпного золота в Амурской области и девятое из 48 предприятий Забайкальского края. Основным видом деятельности является добыча золота на рассыпных месторождениях дражным и раздельным открытым способами добычи, а также извлечение металла из рудного месторождения.

Золотодобывающие подразделения представлены шестью карьерами, обеспеченными полным комплексом необходимого горного технологического оборудования, техники и объектами социально-культурного быта. К вспомогательным цехам, обслуживающим основное производство относятся: цех ремонта горного оборудования, транспортный цех, участок геологоразведочных работ, пробирно-аналитическая лаборатория.

На предприятии работает более 1600 человек, среднемесячная заработная плата составляет около 80 тыс. рублей. Важнейшими приоритетами для Акционерного общества являются снижение негативного воздействия производства на окружающую среду, а также обеспечение безопасного труда работников.

На рис. А1 приложения А представлена организационная структура предприятия.

Основная часть предприятия находится в Тындинском районе, но есть обособленное подразделение в г. Благовещенске, деятельность которого конкретно будет рассматриваться в данной ВКР.

Обособленное подразделение представляет собой офисный комплекс (двухэтажное здание), в котором обособленное подразделение занимает: 5 кабинетов отделов, кабинет директора, кабинет охраны, серверную и служебное помещение. Сам офисный комплекс непосредственно принадлежит АО «Прииск Соловьеский», но в нем также располагаются и другие организации.

В подразделении находятся 5 отделов предприятия:

– отдел материально-технического снабжения (ОМТС);

– бухгалтерия;

– юридический отдел;

– экологический отдел;

– Отдел капитального строительства.

Представленные выше отделы выполняют большое множество функций по своему направлению. Опишем основные из них.

ОМТС:

– организация материально-технического снабжения и обслуживания;

– формирование заказов, составление заявок на приобретение материальных ресурсов;

– согласование с поставщиками изменения условий заключенных договоров;

– организация рационального использования материально-технических ресурсов и т.д.

Бухгалтерия:

– ведение достоверного бухгалтерского, налогового и управленческого учета финансово-хозяйственной деятельности предприятия;

– формирование и сдача бухгалтерской, налоговой и управленческой отчетности финансово-хозяйственной деятельности;

– взаимодействие с государственными налоговыми и иными органами;

– налоговое планирование.

Юридический отдел:

– поиск, сбор, приобретение нормативно-правовых документов, необходимых для осуществления деятельности предприятием;

– организация систематизированного учета и хранения поступающих на предприятие нормативных правовых актов;

– проверка соответствия закону представляемых на подпись руководителю предприятия проектов приказов, инструкций и т.д.

Экологический отдел:

– разработка экологических стандартов и нормативов предприятия;

– создание на предприятии эффективной системы экологической информации, распространяемой на всех уровнях управления.

– проведение экологической экспертизы технико-экономических обоснований, проектов, а также создаваемых новых технологий и оборудования.

– составление перспективных и текущих планов по охране окружающей среды, контроль за их выполнением и т.д.

Отдел капитального строительства:

– разработка проектов долгосрочных, среднесрочных и текущих планов капитального строительства;

– составление титульных списков на все объекты капитального строительства, заявок на строительные материалы и оборудование;

– заключение договоров с проектными организациями и подрядчиками на разработку проектно-сметной документации и строительство объектов;

– согласование графиков проектных и строительных работ и т.д.

Для составления эффективной политики безопасности необходимо подробно рассмотреть и изучить предприятие.

Далее для этого рассмотрим кадровый состав обособленного подразделения.

Таблица 1 – Кадровый состав обособленного подразделения

Должность	Кол-во	Рабочее место
1	2	3
Ген. Директор	1	Кабинет директора
Зам. ген. директора	2	Бухгалтерия
Инженер по охране окр. среды	2	Экологический отдел
Начальник отдела кап. строительства	1	Отдел кап. строительства
Специалист отдела кап. строительства	2	Отдел кап. строительства
Инженер по снабжению	1	ОМТС

Продолжение таблицы 1

1	2	3
Менеджер по подготовке производства	1	Экологический отдел
Юрист	1	Юридический отдел
Бухгалтер	1	Бухгалтерия
Администратор офисного здания	1	ОМТС
Водитель агент по снабжению	1	ОМТС
Охранник	1	Кабинет охраны
Уборщик нежилых помещений	2	Все объекты обособленного подразделения

1.2 Описание аппаратного и программного обеспечения

В обособленном подразделении функционирует большое количество как программного, так и аппаратно-технического обеспечения.

Аппаратное обеспечение: персональные компьютеры (14шт.), принтеры (6шт.), сканер, сервер, камеры видеонаблюдения (3шт.), стационарные телефоны (9шт.), IP телефоны (4шт.), тревожная кнопка, сейфы (3шт.).

Программного обеспечение: Windows 7, Microsoft Office 2013, Антивирус Касперского, Dr.Web, Ccleaner, Google Chrome, Verdox, AutoCAD, TeamViewer, The Bat! Professional, 1С: Бухгалтерия, модуль природопользователя, ARM организация.

На рисунке 1 представлена техническая архитектура сети. Информационная система представляет собой совокупность рабочих станций и сервера, объединенных в единую локальную сеть. Данные хранятся и обрабатываются как на рабочих станциях, так и на файловом сервере. Топология сети – звезда, линии связи сети - неэкранированные витые пары категории 5, сетевые адаптеры сети и коммутаторы Ethernet – 10/100 Base-T.

Проанализировав техническую архитектуру можно, что сеть недостаточно защищена, так как не используются межсетевые экраны.

В данном случае используется маршрутизатор, который не обеспечивает безопасность подключений.

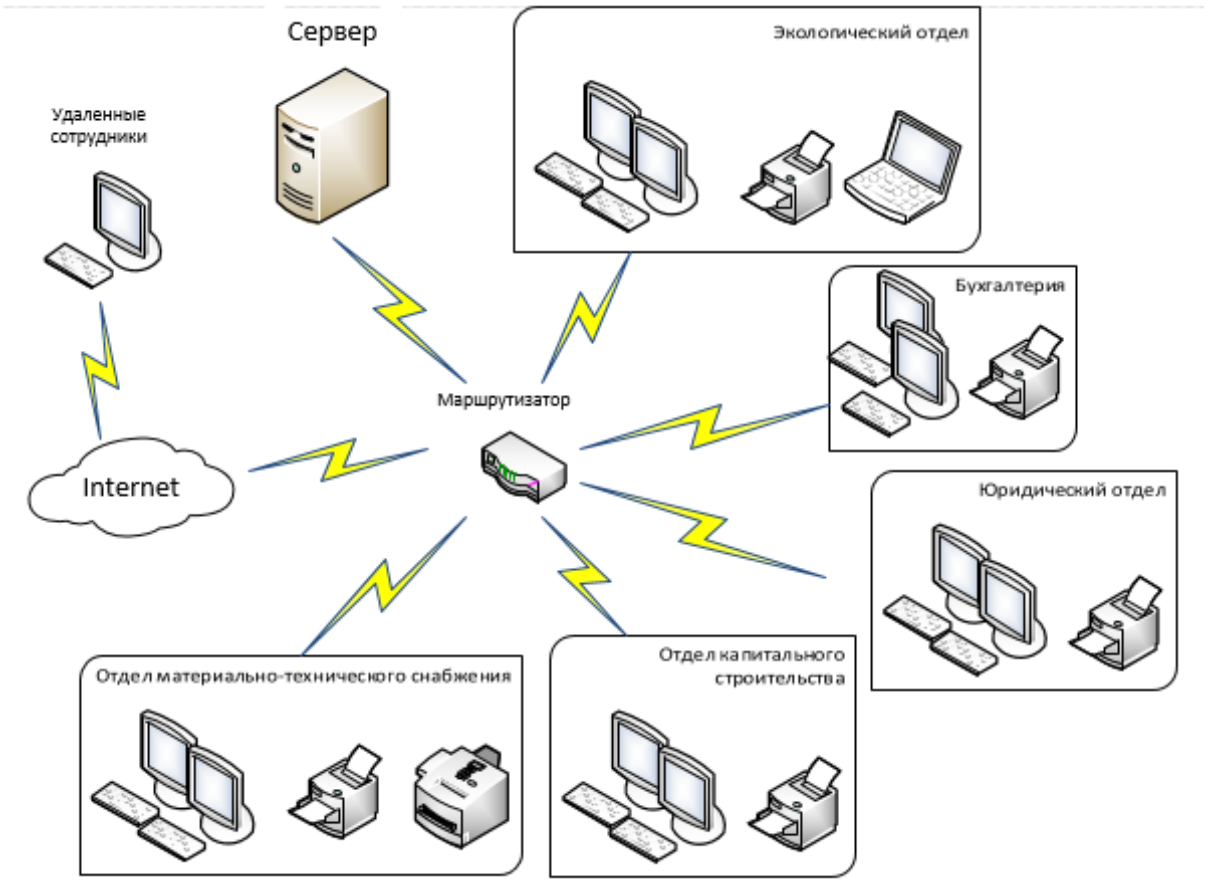

Рисунок 1 – Техническая архитектура ИС

1.3 Информационные потоки предприятия

В обособленном подразделении функционирует большое количество информации. Она передается, отправляется, принимается как внутри самого подразделения, так и между подразделением с другими внешними источниками. Для графического описания функционирования подразделения предприятия, используется программный продукт Ramus.

Внешний документооборот подразделения представлен на рис. Б1, внутренний на рис. Б2 приложения Б.

При исследовании внешнего документооборота можно выделить следующие внешние связи обособленного подразделения с поставщиками, банками, обслуживающими компаниями, государственными органами, с основным предприятием в с. Соловьевск.

Банки, работающие с обособленным подразделением: Сбербанк, ВТБ.

К обслуживающим компаниям относятся:

– «РОС Охрана» (тревожная кнопка), ЧОП «Русич» (охранник, видеонаблюдение) – охрана объекта и территории здания;

– ООО «Системы и решения» – компьютерное обслуживание;

– ООО «Система безопасности» – видеонаблюдение, пожарная сигнализация;

– Teledyne Systems – Internet провайдер.

Под поставщиками понимаются различные компании, имеющие отношения к потребностям предприятия (спецтехника, оборудование, продовольственные товары и т.д.).

К государственным органам относятся: Федеральная налоговая служба, органы судебной власти, прокуратура, гос. комитеты, комиссии и т.д.

Внутренний документооборот представляет собой передачу информации между отделами обособленного подразделения.

1.4 Объект защиты. Перечень информации, подлежащей защите

Выбор объекта и защиты является главным аспектом для разработки политики безопасности.

Под объектом защиты понимается информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации.

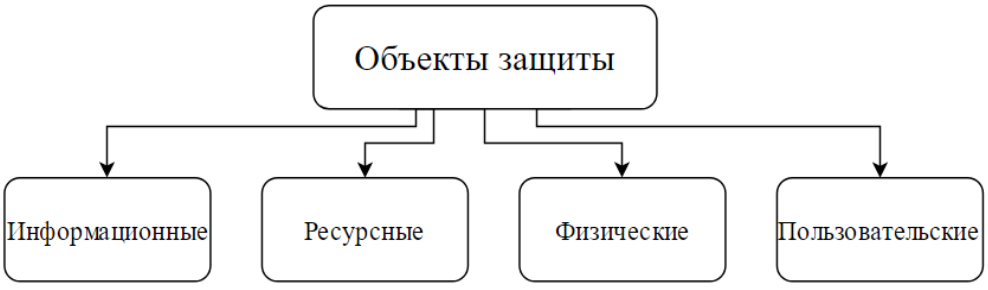

Рисунок 2 – Классификация объектов защиты

К информационным объектам защиты относятся:

− бумажные носители;

− информация в электронном виде;

− цифровые сигналы;

− аналоговые сигналы.

К ресурсным:

− аппаратное обеспечение;

− программное обеспечение;

− процессы обработки информации;

− сервера.

К физическим:

− здание;

− помещение;

− территория;

− техническое оборудование;

− сетевые каналы;

− каналы связи.

К пользовательским:

− персонал;

− пользователи информации;

− собственники информации;

− обслуживающий персонал.

Процессами, подлежащими защите можно обозначить всю деятельность обособленного подразделения, связанную со сбором, обработкой, систематизацией, накоплением, уточнением, использованием, хранением, уничтожением и передачей конфиденциальной информации.

Защите подлежит вся информация и информационные ресурсы предприятия, независимо от их формы представления и местоположения в информационной системе подразделения.

Информацию, функционирующую на предприятии можно разделить коммерческую информацию, персональные данные, а также на общедоступную информацию.

Таблица 2 – Классификация информации по категориям доступа

Тип информации	Описание	Организационно-правовое обеспечение
Коммерческая тайна	Режим конфиденциальности информации, позволяющий ее обладателю при возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить коммерческую выгоду	1. ФЗ РФ от 29.07.2004 N 98-ФЗ «О коммерческой тайне» 2. Постановление Правительства РСФСР от 05.12.1991 N 35 (с изменениями от 03.10.2002)
Персональные данные	Любая информация, относящаяся к прямо или косвенно субъекту персональных данных)	1. ФЗ РФ от 27.07.2006 N 152-ФЗ «О персональных данных» 2. Ст. 86-90 ТК РФ
Общедоступная информация	Информация, доступ к которой нельзя ограничивать	1. ФЗ РФ от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации», ст.7 2. ФЗ РФ от 26.12.1995 N 208-ФЗ «Об акционерных обществах», в статьях 89-92

В соответствие с таблицей 2, составим перечень информации, функционирующей на предприятии.

Рассмотрим сведения, относящиеся к конфиденциальной информации.

Производство, наука, технологии:

– об уровне запасов, материалов и комплектующих, готовой продукции;

– о планах закупок и продаж;

– сведения о планах расширения или свертывания производства;

– нормативно – техническая документация;

– о технологических производственных процессах;

– о структуре, составе, материально-техническом оснащении;

– данные об объемах перевозок, транспортных расходах;

– о перспективных методах управления производством;

– о ключевых идеях НИР;

– об изобретениях, научных, технических, конструкторских и технологических решениях;

– о проектах, схемах, технических решениях;

– о перспективные планы развития предприятия;

– о заявках клиентов;

– о заявках на проведение экспертиз и их результатов;

– о сертификатах;

– о судебных исках, писем, соглашений;

– о данных деятельности отделов;

– о состоянии программного и компьютерного обеспечения и пароли доступа;

– проекты, схемы;

– технические решения;

– формулы, расчеты;

Финансы:

– о планах инвестиций предприятия;

– о данных в бухгалтерских регистрах, книгах Общества;

– о финансовых операциях;

– о внешнем и внутреннем финансировании;

– договора купли-продажи акций;

– о документах об уплате налогов и платежах;

– счета, накладные;

Переговоры, совещания, контракты:

– о подготовке и результатах проведения переговоров;

– о получаемых заказах и предложениях;

– о результатах коммерческих переговоров и условиях;

– об условиях по сделкам и соглашениям;

– о фактах проведения и целях совещаний и заседаний;

– о предмете и результатах совещаний органов управления;

– о подготовке и результатах;

– о переговорах с деловыми партнерами компании;

– о лицах, ведущих переговоры, руководстве фирм, их характеристиках;

Сведения, относящиеся к персональным данным.

Личные данные сотрудников, поставщиков, покупателей, контрагентов, посредников, спонсоров, партнеров, акционеров, соискателей работы, бывших сотрудников (Ф.И.О., возраст, адрес, телефон, семейное положение, паспортные реквизиты, ксерокопия свидетельства пенсионного госстраха, ксерокопия диплома, сведения о трудовой деятельности, сведения о воинском учете, ИНН, сведения о соц. льготах).

Сведения, относящиеся к общедоступной информации.

– сайт предприятия;

– расположение производственных объектов;

– руководство предприятия;

– ИНН, ОКПО;

– юридический, почтовый адрес, контакты (телефон, факс, эл. почта);

– политика в области промышленной безопасности;

– сведения о предстоящих собраниях акционеров;

– годовой отчет общества, годовую бухгалтерскую отчетность;

– сведения, дающие право на осуществление предпринимательской деятельности;

– о численности и составе работников;

– о задолженности по выплате заработной платы;

– о нарушениях законодательства РФ и фактах привлечения к ответственности за совершение этих нарушений;

– о перечне лиц, имеющих право действовать без доверенности от имени Общества.

Данные, относящиеся к коммерческой тайне и персональным данным хранятся в электронном и бумажном виде. Данные размещаются в базах данных, сетевых ресурсах, в системе электронного документооборота «Verdox», «The Bat! Professiaonal». Бумажные носители конфиденциальной информации хранятся в сейфах.

Общедоступные сведения свободно представлены в сети Internet.

2 АНАЛИЗ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1 Идентификация и оценка информационных активов

Актив – это ресурс, который имеет ценность для предприятия, обеспечивающий функционирование деловых операций и непрерывность бизнеса. Актив является важным компонентом или частью общей системы и поэтому нуждается в защите со стороны предприятия.

Для дальнейшего анализа системы ИБ предприятия, необходимо идентифицировать и оценить важность его основных активов.

В таблице 3 представлены основные активы обособленного подразделения предприятия, имеющие наиболее высокую ценность.

Ценность актива определяется по 5-тибальной шкале (где 5 – наибольшая степень ценности актива), в зависимости от затрат, принесенных по причине утраты конфиденциальности, целостности и доступности из-за произошедшего инцидента.

Таблица 3 – Оценка информационных активов

Актив	Ценность	Обоснование выбора актива
1	2	3
Док-ты	5	К ним относятся: коммерческая тайна, персональные данные, конфиденциальная и другая, имеющая ценность информация, отображенная на бумажных носителях и в электронном виде
Сервер	5	Большая часть жизненно важной информации предприятия находится именно на серверах
БД	5	Инструмент для сбора и структурирования информации, в котором хранится информация предприятия
ПК	4	Имеет важность для предприятия так как он представляет аппаратное средство, которое используется для создания, обработки, хранения, передачи информации

Продолжение таблицы 3

1	2	3
Помещение	3	Место хранения всех активов подразделения
Каналы передачи данных	2	Имеют важность так как являются средствами двухстороннего обмена данными предприятия, которые включают в себя линии связи и аппаратуру передачи (приема) данных
ПО	4	Совокупность программ, позволяющих осуществить на компьютере автоматизированную обработку информации предприятия
Сейфы	1	Хранилище предметов, документов, имеющих важность для предприятия

Активы, имеющие наибольшую ценность:

– документы;

– сервер;

– БД;

– ПК;

– ПО.

2.2 Уязвимости информационной безопасности

В данном разделе проведен анализ и оценка уязвимостей предметной области (таблица 4), которые могли бы быть использованы источником угроз для нанесения ущерба активам и деятельности предприятия.

Уязвимость – это недостаток программного (программно-технического) средства или информационной системы в целом, которым (которая) может быть использована для реализации угроз безопасности информации.

Одним из важнейших механизмов защиты является поиск и устранение уязвимостей, так как, именно, с помощью недостатков ИС, нарушитель производит атаку.

Уязвимости разделены на виды, представленные на рисунке 3.

Рисунок – 3 Классификация уязвимостей

Необходимо найти и оценить уязвимость объектов защиты ИС, для этого рассмотрим классификацию уязвимостей по уровню риска.

– высокий (В) – нарушитель может осуществлять полный контроль над атакуемым объектом;

– средний (С) – нарушитель может получить информацию, которая с высокой степенью вероятности позволит получить полный контроль над объектом;

– низкий (Н) – нарушитель может осуществлять сбор критической информации о системе.

Представленная выше классификация используется для оценки уровня риска уязвимостей при определении качества защищенности ИС. Она достаточно условна, соответственно, это субъективный метод классификации уязвимостей.

Таблица 4 – Оценка уязвимостей ИБ

Уязвимости	Наименование актива				
	Докты	Сервер	БД	ПК	ПО
1	2	3	4	5	6
1.Инфраструктура					
Отсутствие физической защиты зданий, дверей и окон	Н	Н	Н	Н	Н
Неправильное использование физических средств управления доступом в помещения	С	С	Н	В	Н
Нестабильное электропитание	С	С	С	С	С

Продолжение таблицы 4

1	2	3	4	5	6
Размещение в зонах возможного затопления	Н	Н	Н	Н	Н
2.Аппаратное обеспечение					
Колебания напряжения	Н	Н	С	Н	С
Подверженность воздействию влаги, пыли, загрязнения	Н	С	Н	С	Н
Подверженность температурным колебаниям	Н	С	Н	С	Н
Отсутствие контроля замены оборудования	Н	С	Н	С	Н
Недостаток аппаратного обеспечения для безопасности помещений	Н	Н	С	Н	С
3.Программное обеспечение					
Уязвимости средств антивирусной защиты и контроля доступа	С	С	С	В	В
Сложный пользовательский интерфейс	С	Н	Н	Н	В
Отсутствие механизмов идентификации и аутентификации	С	Н	С	Н	Н
Неконтролируемая загрузка и использование программного обеспечения	Н	Н	С	С	Н
Отсутствие эффективного контроля внесения изменений	С	Н	Н	Н	С
Отсутствие документации	С	Н	С	Н	С
Отсутствие резервных копий	С	Н	С	Н	Н
Невыполнение или выполнение в недостаточной мере тестирования	С	Н	С	С	С
Списание или повторное использование запоминающих сред без надлежащего стирания записей	Н	Н	Н	Н	Н
Отсутствие обновлений	Н	Н	Н	Н	С
4.Коммуникации					
Незащищенные линии связи	С	Н	Н	Н	Н
Незащищенные подключения к сетям общего пользования	Н	Н	С	Н	С
Неадекватное управление сетью	С	Н	С	Н	С
Незащищенные потоки конфиденциальной информации	С	Н	Н	Н	Н
Пересылка паролей открытым текстом	Н	Н	Н	Н	Н

Продолжение таблицы 4

1	2	3	4	5	6
Отсутствие идентификации и аутентификации отправителя и получателя	С	Н	Н	Н	Н
Отсутствие контроля входных и выходных данных	С	Н	Н	Н	Н
Коммутируемые линии	Н	Н	Н	Н	Н
5.Документы					
Отсутствие проверки обрабатываемых данных	Н	Н	Н	Н	Н
Хранение в незащищенных местах	В	Н	С	Н	С
Недостаточная внимательность при уничтожении	В	Н	С	Н	С
Неконтролируемое копирование	В	Н	Н	Н	Н
6.Персонал					
Отсутствие персонала	С	С	С	С	С
Отсутствие надзора за работой обслуживающих компаний, приглашенного персонала	С	С	Н	С	Н
Недостаточная подготовка персонала по вопросам обеспечения безопасности	С	С	С	С	С
Неправильное использование программно-аппаратного обеспечения	С	Н	С	С	С
Несоответствующие процедуры набора кадров	С	Н	Н	Н	Н
Отсутствие политики правильного пользования телекоммуникационными системами для обмена сообщениями	Н	Н	Н	Н	Н
Отсутствие механизмов отслеживания	Н	Н	Н	Н	Н
Отсутствие политики безопасности	С	Н	Н	Н	Н
Немотивированный или недовольный персонал	С	Н	Н	Н	Н
Нет отмены прав доступа при увольнении	С	Н	С	Н	Н

2.3 Угрозы информационной безопасности

В стандарте, под угрозой понимается потенциальная причина нежелательного инцидента, результатом которого может быть нанесение ущерба системе или организации.

Существует огромное множество видов классификаций угроз информационной безопасности. Мы остановимся на следующей классификации:

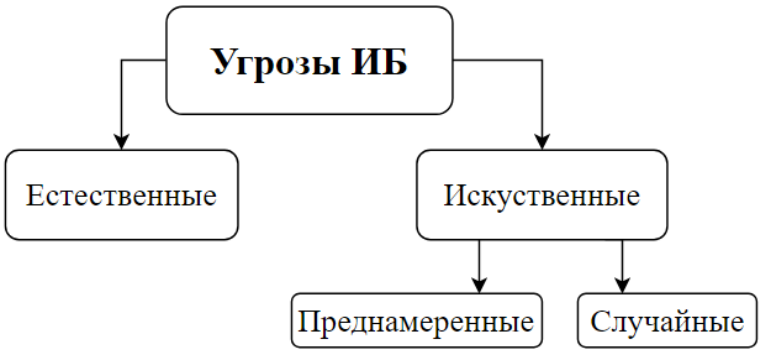

Рисунок 4 – Классификация угроз

Для оценки вероятности реализации угрозы используем классификацию:

– низкая вероятность (Н) – угроза осуществится, не существует инцидентов, статистики, мотивов и т.п., которые указывали бы на то, что это может произойти. Ожидаемая частота реализации угрозы не превышает 1 раза в 5-10 лет;

– средняя вероятность (С) – угроза осуществится (в прошлом происходили инциденты), или существует статистика, указывающая на то, что такие или подобные угрозы иногда осуществлялись прежде, или существуют признаки того, что у атакующего могут быть определенные причины для реализации таких действий. Ожидаемая частота реализации угрозы – примерно один раз в год.

– высокая вероятность (В) – угроза, скорее всего, осуществится. Существуют инциденты, статистика, указывающая на то, что угроза, скорее всего, осуществится, или могут существовать серьезные причины или мотивы для атакующего, чтобы осуществить такие действия. Ожидаемая частота реализации угрозы – еженедельно или чаще.

Таблица 5 – Оценка угроз ИБ

Угроза ИБ	Наименование актива				
	Док-ты	Сер-вер	БД	ПК	ПО
1	2	3	4	5	6
1.Преднамеренные (угрозы, вызванные деятельностью человека с корыстными, идейными и другими целями)					
Хищение	С	С	Н	С	Н
Перехват информации	С	Н	Н	Н	Н

Продолжение таблицы 5

1	2	3	4	5	6
Нелегальное проникновение злоумышленников	Н	Н	Н	Н	Н
Внедрение вредоносного ПО	С	В	С	В	В
Незаконное подключение к линиям связи	Н	Н	Н	Н	Н
Подделка электронной подписи	С	Н	Н	Н	Н
Подкуп, шантаж и другие пути воздействия на персонал	Н	Н	Н	Н	Н
Пожар	Н	Н	Н	Н	Н
Затопление	Н	Н	Н	Н	Н
Изменение маршрута направления сообщений	С	Н	Н	Н	Н
НСД к ПО	С	Н	С	Н	В
Перегрузка трафика	Н	С	Н	Н	Н
НСД к сетям	С	В	С	Н	Н
Раскрытие информации	С	Н	С	Н	Н
Искажение в информации	С	Н	С	Н	Н
Применение подслушивающих устройств	С	С	С	С	С
Несанкционированное копирование носителей информации	С	Н	Н	Н	Н
Умышленная порча или вывод из строя оборудования	Н	С	Н	С	Н
2.Случайные (угрозы, вызванные деятельностью человека, ошибками в проектировании, в программном обеспечении, ошибки персонала)					
Затопление	Н	Н	Н	Н	Н
Пожар	Н	Н	Н	Н	Н
Неумышленная порча, вывод из строя оборудования	Н	С	Н	С	Н
Ошибка обслуживающего персонала	В	Н	С	С	Н
Неумышленная порча носителей информации	С	Н	Н	Н	Н
Направление сообщений по ошибочному адресу	С	Н	Н	Н	Н
Непреднамеренное заражение компьютера вирусами	С	Н	С	В	В
Неумышленное отключение оборудования	Н	С	Н	С	Н
Использование программ, которые не нужны для выполнения должностных обязанностей	В	Н	С	В	В
Ввод ошибочных данных	С	Н	С	Н	Н
Неосторожные действия, влекущие за собой разглашение конфиденциальной информации	С	Н	Н	Н	Н
Неумышленная порча носителей информации	С	Н	Н	Н	Н

Продолжение таблицы 5

1	2	3	4	5	6
Утрата, передача или разглашение идентификаторов, к которым относятся пароли, ключи шифрования	С	Н	Н	Н	Н
3.Естественные (вызванные воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека)					
Затопление	Н	Н	Н	Н	Н
Колебания напряжения	С	С	С	Н	Н
Воздействие пыли	Н	С	Н	С	Н
Ухудшение состояния, износ носителей данных	С	Н	Н	Н	Н
Перегруженный трафик	В	С	В	Н	С
Сбои в функционировании услуг связи	С	Н	С	Н	С
Сбой ПО	С	Н	С	Н	С
Технические неисправности сетевых компонентов	С	С	С	Н	С

Основными угрозами безопасности, имеющие наибольший риск являются:

− НСД к данным;

− халатность служащих;

− вирусные атаки;

− съем информации с использование технических средств;

− хищение;

− спам;

− сбои аппаратуры и ПО.

2.4 Модель нарушителя

Всех нарушителей можно разделить на две основные группы: внутренние и внешние.

Под внутренними нарушителями подразумеваются все работники объекта информатизации, имеющие санкционированный доступ на территорию объекта к ресурсам обособленного подразделения предприятия. Под внешними нарушителями подразумеваются все остальные лица.

Также нарушителей можно разделить на две категории:

I – лица, не имеющие права доступа в контролируемую зону;

II – лица, имеющие право доступа в контролируемую зону.

К внешним нарушителям можно отнести:

– нарушители пропускного режима;

– уволенные сотрудники;

– сотрудники органов ведомственного надзора и управления;

– представители конкурирующих организаций;

– приглашенные посетители;

– клиенты.

К внутренним нарушителям можно отнести:

– обслуживающий персонал (системные администраторы, администраторы АС, администраторы баз данных, инженеры, уборщицы, охранники);

– работники-программисты, сопровождающие системное, общее и прикладное программное обеспечение;

– другие работники структурных подразделений, имеющие санкционированный доступ на объект;

– сотрудники службы безопасности.

2.5 Средства защиты информации на предприятии

Средства защиты информации – это совокупность инженерно-технических, электрических, электронных, оптических устройств и приспособлений, приборов и технических систем, применяемых для обеспечения безопасности ЗИ

Средства защиты информации по способу реализации можно разделить на группы:

– физические средства;

– программные средства;

– организационные средства.

2.5.1 Физические средства защиты

В офисном комплексе, помимо обособленного подразделения, также находятся другие организации, что создает угрозу безопасности, а именно доступ посторонних лиц.

Для обеспечения безопасности в обособленном подразделении используется охранная система, которая включает в себя следующие объекты: кабинет охраны, охранник, тревожную кнопку, обслуживающие компании, контролирующие безопасность помещений, здания и прилегающей к ней территории.

Также используется система видеонаблюдения, включающая три купольные камеры. Первая находится на въезде на территорию офисного комплекса. Вторая при подъеме на второй этаж и третья в коридоре на втором этаже. Данного количества камер недостаточно для просмотра всего периметра помещения, что может быть отражено на угрозах доступа в кабинеты.

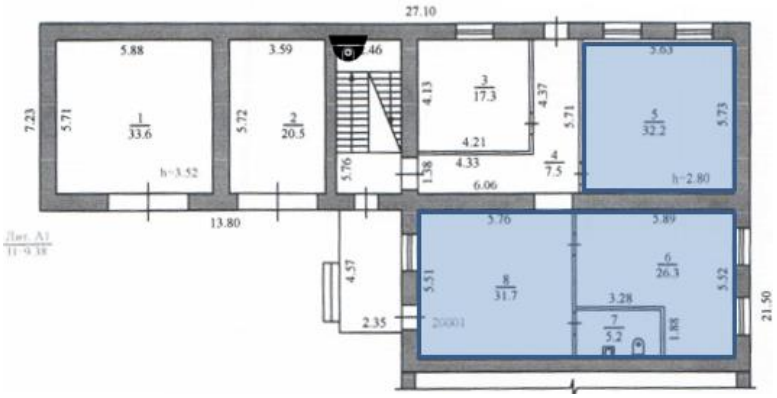

Рисунок 5 –Расположение камер на первом этаже

Рисунок 6 – Расположение камер на втором этаже

Все кабинеты закрываются на ключ, ключи хранятся в кабинете охраны. Также в качестве физических средств защиты можно выделить сейфы, с целью предотвращения потерь информации используется противопожарная система.

При анализе технической архитектуры, выявлен недостаток – отсутствие сертифицированных межсетевых экранов, обеспечивающих защиту и контроль взаимодействия ЛВС организации с сетями общего доступа.

Серверное оборудование ЛВС размещено в специально оборудованной аппаратной комнате, в техническом помещении офиса, находящегося в пределах видеонаблюдения.

2.5.2 Программные средства защиты

К программным средствам можно отнести антивирусную защиту, установленную на все ПК подразделения. В качестве антивирусного продукта используется лицензионный Kaspersky Internet Security, который постоянно обновляется.

Совместно с ним используются утилиты Dr.Web, Ccleaner для поиска и устранения угроз, очистки свободного места.

При работе с специализированными программами для обмена информации, осуществляется парольная аутентификация.

Также используется программа «The Bat! Professional», которая защищает передачу информацию от перехвата третьими лицами.

Используется лицензионное программное обеспечение, которое постоянно обновляется.

2.5.3 Организационные средства защиты

К организационным средствам защиты, использующимся на предприятии можно отнести:

– организация внутри объектового режима и охраны;

– ограничение доступа к помещениям, где информация содержится и обрабатывается;

– хранение информации в закрытых, для посторонних, сейфах.

Комплексная система доступа к информационным ресурсам не разработана.

Действия пользователей и администраторов не регламентированы соответствующими инструкциями.

2.6 Оценка рисков

Для оценки рисков ИБ был выбран метод, представленный в источнике, а именно детальный анализ риска.

Целью детального анализа рисков является возможность выбора обоснованных защитных мер.

Для определения величины риска, необходимы:

– оценка информационных активов (таблица 3);

– оценка уязвимостей ИБ (таблица 4);

– оценка угроз ИБ (таблица 5);

– средства защиты информации.

Также для количественной оценки риска, используется таблица 6. С помощью нее, для каждого актива определяется риск в баллах.

Таблица 6 – Количественная оценка рисков

Ценность актива	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровень уязвимости								
	Н	С	В	Н	С	В	Н	С	В
1	0	1	2	1	2	3	2	3	4
2	1	2	3	2	3	4	3	4	5
3	2	3	4	3	4	5	4	5	6
4	3	4	5	4	5	6	5	6	7
5	4	5	6	5	6	7	6	7	8

Суть такого подхода заключается в определении наиболее критичного актива с точки зрения рисков ИБ, оцененных по баллам.

Для каждого актива рассматривают уязвимые места и соответствующие им угрозы. Если есть уязвимые места без соответствующей угрозы или наоборот, риск отсутствует.

Затем идентифицируют соответствующий ряд матрицы по ценности актива, а соответствующую колонку – по степени угрозы и уязвимости.

Например, возьмем актив «Сервер», ценность актива равна 5, затем определим угрозу, например, «Хищение», которая оценивается как «средняя», и соответственно уязвимость «Недостаточная подготовка персонала по вопросам обеспечения безопасности» характеризуют, как «среднюю», следовательно, ранг риска равен 6.

Баллы каждого риска актива суммируются, затем ранжируются.

Основываясь на данном методе, определим ранг риска, представим в таблице 7.

Таблица 7 – Результаты оценки рисков информационных активов

Риск (в баллах)	Актив	Ранг риска
203	Документы	1
191	БД	2
188	Сервер	3
149	ПО	4
145	ПК	5

2.7 Рекомендации по обеспечению ИБ

Проанализировав систему ИБ обособленного подразделения, можно сказать, что основными угрозами ИБ являются: НСД к активам, хищение, ошибки персонала, сбои аппаратного и программного обеспечения, заражение вирусами, перехват, удаление, раскрытие, искажение, конфиденциальной информации и др. Все эти угрозы могут быть реализованы в связи с большим количеством уязвимостей.

Для того, чтобы минимизировать эти угрозы, необходимо выделить следующие рекомендации:

Рекомендации по физической защите.

Увеличить количество камер, как на первом, так и на втором этаже, для увеличения обзора и контроля помещений подразделения.

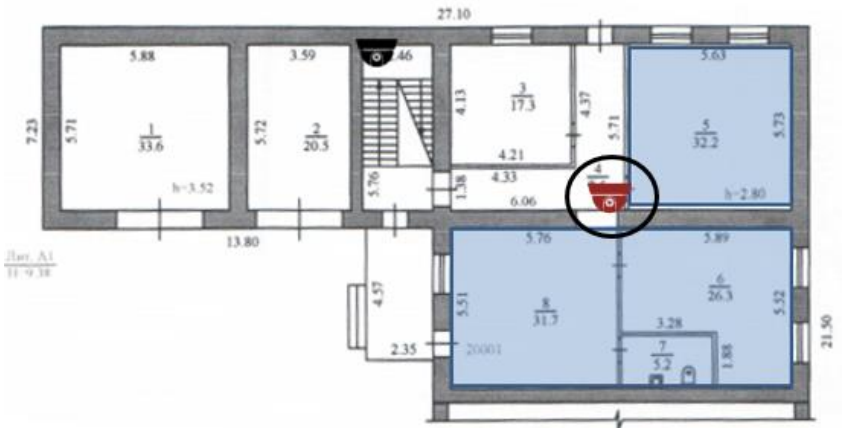

Рисунок 7 – Расположение дополнительных камер на первом этаже

Рисунок 8 – Расположение дополнительных камер на втором этаже

Например, МВК-MV720 Ball (2,8-12) – купольная видеокамера, 2765 руб., режимы День/Ночь, ИК-подсветка до 20, механический автоматический ИК-фильтр.

Ввести контрольно-пропускную систему на базе турникета, что позволит обеспечить безопасность объекта, регистрировать посетителей, контролировать действия охранников, разграничить доступ, а также учитывать рабочее время сотрудников. (Например, электронная проходная система Carddex «STR 02» – турникет со встроенным контроллером стоимость, 35000 руб., автономный режим прохода по картам, надежный блокирующий механизм, длительная безотказная работа).

Также необходимо установить в каждый кабинет инфракрасные датчики движения, так как обособленное подразделение находится на первом и втором этаже, что создает угрозу проникновения в здание. Решетки на окнах отсутствуют. Только одна половина здания оснащена ограждением с закрывающимися воротами. (Например, «Фотон-9» (ИО409-8) – датчик инфракрасный охранный используется для обнаружения проникновения в охраняемое помещение и формирования извещения о проникновении. Цена 585 руб.).

Рекомендации по аппаратно-технической защите.

Обеспечить использование межсетевых экранов для защиты ЛВС.

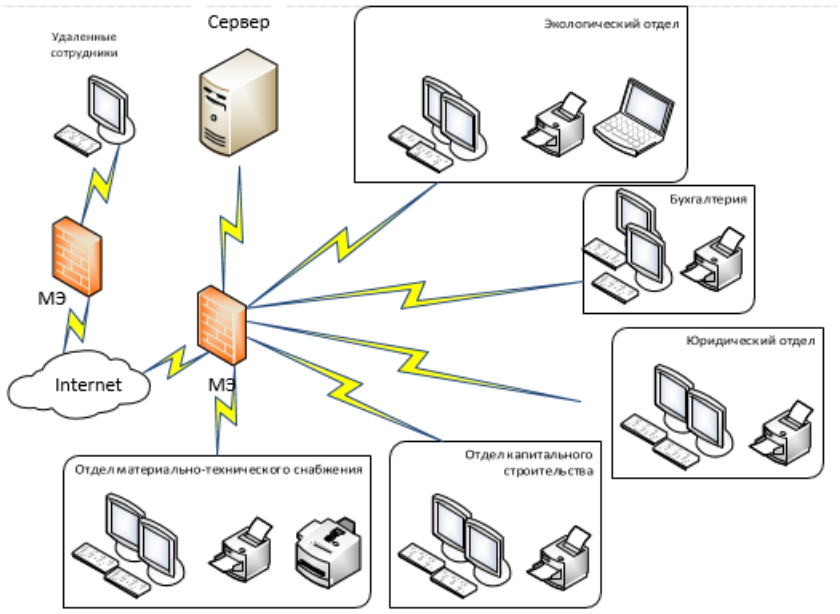

Рисунок 9 – Схема защищенной технической архитектуры

Например, межсетевой экран Cisco ASA5506-K8, 32000 руб., 8 портов типа 10/100/1000 Base-TX (1000 Мбит/с), порт USB 2.0, пропускная способность 750 Мбит/с, максимальное количество одновременных сессий 20000. Устройство позволит обеспечить безопасность сети, путем мониторинга, входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик.

Необходима закупка и установка источников бесперебойного питания для обеспечения сотрудникам своевременного сохранения текущих документов во избежание потери данных в условиях отключения электричества для повышения

надежности хранения информации. (Например, 3Cott 600VA-3SE 360W AVR – ИБП, осуществляющий защиту локальной сети, а также комплексом защит, которые включают в себя защиту от короткого замыкания, защиту от перегрузки, от высоковольтных импульсов и фильтрацию помех, цена 1900).

Так как в кабинете директора проводятся различные совещания, переговоры необходимо защитить помещение от утечки информации. Для этого можно использовать генератор шума по цепям электропитания, заземления и ПЭМИ, он обеспечивает защиту информации от утечки, путем создания на границе контролируемой зоны широкополосной шумовой электромагнитной помехи. (Например, ЛГШ-503, стоимость около 30.000 руб., имеет сертификаты ФСТЭК России, санитарно-эпидемиологическое заключение и сертификат ГОСТ Р).

Рекомендации по программной защите.

Необходимо следить за обновлением программного обеспечения, а также антивирусной защиты.

Для поиска и гарантированного уничтожения информации на дисках, необходимо использовать специализированные программы. (Например, «TERRIER» 1700 руб.).

Для контроля защищенности информации также используют системы анализа программного и аппаратного обеспечения TCP/IP сетей. (Сканер-ВС - ПО для комплексного тестирования защищенности информационных систем. Цена: 700 – 1 000 руб.).

Также необходимо использовать средства защиты информации от несанкционированного доступа. (СЗИ от НСД Страж NT, защита информации на рабочих станциях и серверах, контроль утечек и каналов распространения защищаемой информации, 7.000).

Использовать только лицензионное ПО.

Сканировать компьютер, не перезагружать ненужными файлами.

Интернет должен использоваться только для работы.

По организационной защите:

Не допускать нахождение посторонних лиц в помещениях, в которых ведутся работы с секретной и конфиденциальной информацией. Если посторонние лица все же были допущены (уборщицы, ремонтники, и другие сотрудники обслуживающих компаний), то следует следить за ними, во избежание утечки информации.

Назначить персонал по обеспечению информационной безопасности.

Проводить информирование сотрудников в области информационной безопасности.

Важную роль в обеспечении ИБ несет организационно-распорядительная документация, а именно, политика безопасности, которую подробно рассмотрим в следующей главе.

2.8 Обоснование экономической эффективности проекта

2.8.1 Обоснование выбора методики расчёта

В данном дипломной работе будет рассматривается методика оценки совокупной стоимости владения (ССВ) применительно к системе ИБ.

Эта методика применима в случаях, когда используется подход к обоснованию затрат на ИБ.

Методика ССВ позволяет рассчитать всю расходную часть информационных активов компании, включая прямые и косвенные затраты на аппаратно-программные средства, организационные мероприятия, обучение и повышение квалификации сотрудников, реорганизацию, реструктуризацию бизнеса и т. д.

Данная методика может быть использована для доказательства экономической эффективности существующих систем защиты информации.

Таким образом, показатель ССВ можно использовать как инструмент для оптимизации расходов на обеспечение требуемого уровня защищенности ИС и обоснование бюджета на ИБ.

В целом методика ССВ позволяет:

– получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения системы защиты информации;

– оптимизировать инвестиции на ИБ компании с учетом реального значения показателя ССВ.

Основные положения данной методики:

ИБ обеспечивается комплексом мер на всех этапах жизненного цикла ИС, совокупная стоимость владения для системы ИБ в общем случае складывается из стоимости:

– проектных работ;

– закупки и настройки программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и т.д.;

– затрат на обеспечение физической безопасности;

– обучения персонала;

– управления и поддержки системы (администрирование безопасности);

– аудита ИБ;

– периодической модернизации системы ИБ.

Проведем расчет, используя следующую эмпирическую зависимость ожидаемых потерь (рисков) от i-й угрозы информации:

$$Ri = 10(Si + Vi – 4),$$

где Si – коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы, Vi – коэффициент, характеризующий значение возможного ущерба при ее возникновении.

При выполнении дипломного проекта необходимо использовать следующие значения коэффициентов Si и Vi, приведенные в таблице 8.

Таблица 8 – Значения коэффициентов Si и Vi

Ожидаемая (возможная) частота появления угрозы	Предполагаемое значение Si
1	2
Почти никогда	0
1 раз в 1 000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3

Продолжение таблицы 8

1	2
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1-2 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7
Значение возможного ущерба при проявлении угрозы, руб.	Предполагаемое значение Vi
30	0
300	1
3 000	2
30 000	3
300 000	4
3 000 000	5
30 000 000	6
300 000 000	7

Ri1 = = 100 000

Ri2 = = 100 000

Ri3 = = 100 000

Ri4 = = 10 000

Ri5 = = 100 000

Теперь определим суммарную величину потерь по формуле:

$$R = \sum_{i=1}^{N} Ri$$

R = 410 000 (руб.)

Полученные значения приведены в таблице 9.

Таблица 9 – Величины потерь до внедрения/модернизации СЗИ

Актив	Угроза	Величина потерь (руб.)
Документы	НСД к данным, Хищение	100 000
Сервера	Сбои, Хищение, Вирусные атаки	100 000
БД	НСД к данным, Вирусные атаки	100 000
ПК	Халатность служащих, Вирусные атаки	10 000
ПО	НСД к данным, Спам, Сбои, Вирусные атаки	100000
Суммарная величина потерь		410 000

2.8.2 Расчёт показателей экономической эффективности проекта

Для определения экономической эффективности системы защиты информации предприятия необходимы следующие данные (показатели):

– расходы (выделенные ресурсы) на создание/модернизацию данной системы и поддержание её в работоспособном состоянии;

– величины потерь (рисков), обусловленных угрозами информационным активам после внедрения/модернизации системы защиты информации;

Данные по ресурсам необходимым для ИБ представлены в таблицах 10, 11.

Таблица 10 – Содержание и объем ресурса, выделяемого на ЗИ, организационные мероприятия

Организационные мероприятия			
Выполняемые действия	Среднечасовая з/п специалиста (руб.)	Трудоемкость операции (чел. час)	Стоимость, (руб.)
Закупка СЗИ	300	8	2 400
Монтаж и установка аппаратных и программных СЗИ	200	24	4 800
Настройка и отладка установленных средств ИБ	300	8	2 400
Проведение занятий по обучению и использованию СЗИ с сотрудниками отдела	350	4	1 400
Контроль и мониторинг работоспособности СЗИ	150	88	13 200
Физическая охрана помещений, где установлены СЗИ	200	22	3400
Своевременное обслуживания программных и аппаратных СЗИ	350	4	1400
Стоимость проведения организационных мероприятий, всего			29000

Таблица 11 – Содержание и объем ресурса, выделяемого на ЗИ, инженерно-технические мероприятия

Инженерно-технические мероприятия			
Номенклатура	Стоимость, (руб.)	Кол-во (ед. измерения)	Стоимость, (руб.)
1	2	3	4
Купольная видеокамера МВК MV720 Ball	2765	2	5 530
Электронно-проходная система Carddex «STR 02»	35000	1	35000

Продолжение таблицы 11

1	2	3	4
Датчик инфракрасный «Фотон-9» (ИО409-8)	585	5	2925
Межсетевой экран Cisco ASA5506-K8	32000	1	32000
ИБП 3Cott 600VA-3SE 360W	1900	14	26600
Генератор шума ЛГШ-503	25000	1	25000
«TERRIER»	1700	1	1700
Страж NT	7000	5	35000
Сканер-ВС	700	1	700
Стоимость мероприятий инженерно-технической защиты			164455
Объем ресурса, выделяемого на ЗИ			193655

Суммарное значение ресурса, выделяемого на защиту информации исходя из расчетов, составил: 193655 (руб.)

Рассчитанная величина ущерба составила: 410 000 (руб.)

Прогнозируемые данные о величине потерь (рисков) для критичных информационных ресурсов после внедрения/модернизации системы защиты информации приведены в таблице 11.

Таблица 12 – Прогнозируемые величины потерь (рисков) для информационных активов после внедрения системы ЗИ

Актив	Угроза	Величина потерь (руб.)
Документы	НСД к данным, Хищение, Халатность служащих	50 000
Сервера	Сбои, Хищение, Вирусные атаки	10 000
БД	НСД к данным, Вирусные атаки	10 000
ПК	Халатность служащих, Вирусные атаки	1 000
ПО	НСД к данным, Спам, Сбои, Вирусные атаки	10 000
Суммарная величина потерь		81 000

После принятия обязательных допущений о неизменности частоты появления угроз, а также о неизменном уровне надежности созданной системы защиты информации, возможно, определить срок окупаемости системы (Ток). Это выполняется аналитическим способом, с использованием приведенной ниже формулы:

Ток = R∑ / (Rср – Rпрогн),

где (R∑) – суммарное значение ресурса выделенного на защиту информации =193655; (Rср) – объем среднегодовых потерь предприятия из-за инцидентов информационной безопасности в периоде одного года до введения СЗИ = 410 000; (Rпрогн) – прогнозируемый ежегодный объем потерь, после введения СЗИ = 81 000;

Ток = 193655 / (410 000 - 81 000) = 193655 / 329 000 = 0,6 (года).

Также необходимо оценить динамику величин потерь за период не менее 1 года:

Таблица 13 – Оценка динамики величин потерь

	1 кв.	2 кв.	3 кв.	1 год
До внедрения СЗИ	102 500	205 000	307 500	410 000
После внедрения СЗИ	20 250	40 500	60 750	81 000
Снижение потерь	82 250	164 500	246 750	329 000

Графическое представление о динамике потерь:

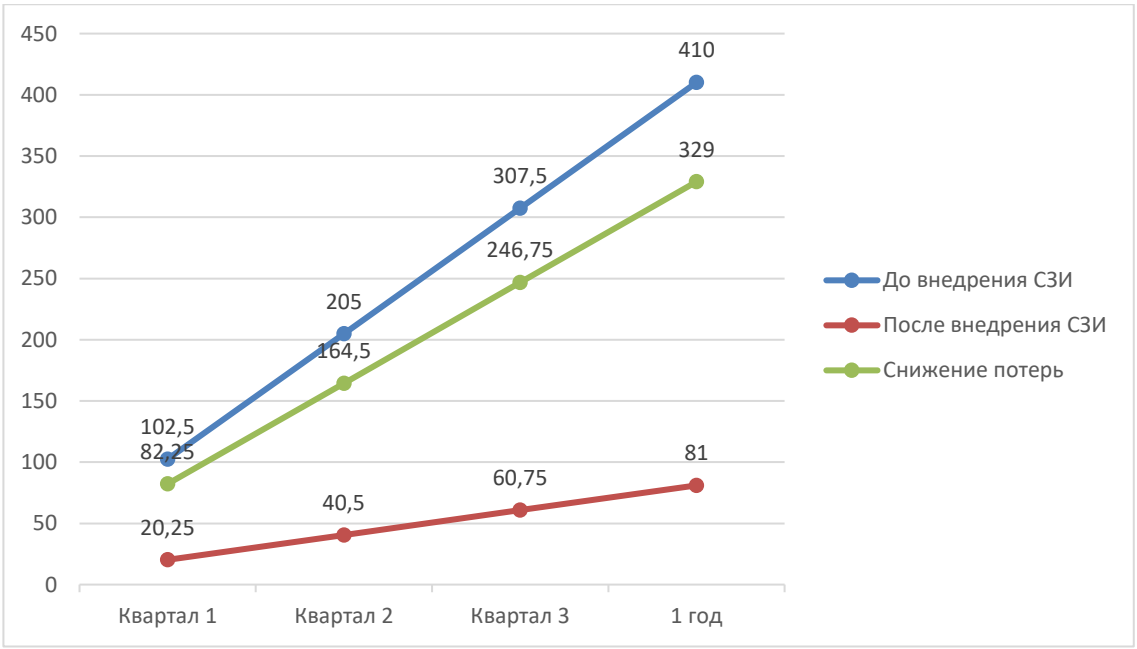

Рисунок 10 - Диаграмма динамики потерь.

3 РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Политика безопасности – это набор норм, правил и практических приемов, которые обеспечивают управление, защиту и распределение ценной информации.

В более широком смысле понятие ПБ определяется как, совокупность документированных административных решений, которые обеспечивают безопасность информационных активов.

Результатом политики является высокоуровневый документ, который представляет собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности предприятия.

Эффективную политику безопасности, можно создать если следовать алгоритму, изображенному на рисунке 11.

Данный алгоритм позволяет поэтапно проанализировать систему ИБ, проанализировать риск, выбрать соответствующие защитные меры, и соответственно, грамотно составить политику ИБ.

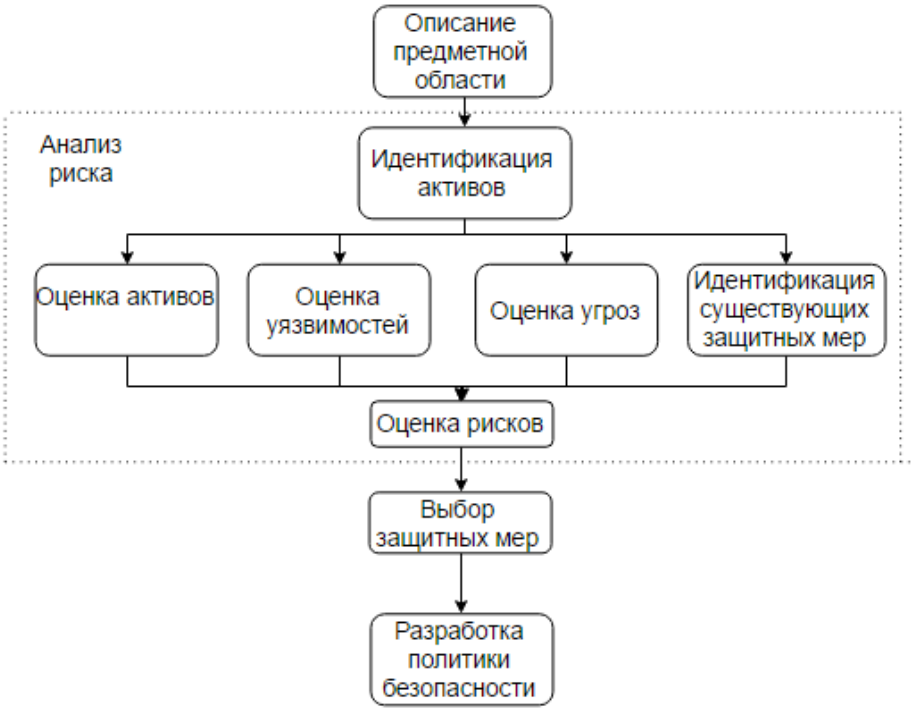

Рисунок 11 – Алгоритм разработки политики безопасности

Все этапы алгоритма были выполнены в главе 2, поэтому можно перейти к составлению самой ПБ.

Существует много решений по созданию ПБ. Эффективной и более подробной, считается многоуровневая ПБ, строение которой представлено на рисунке 12.

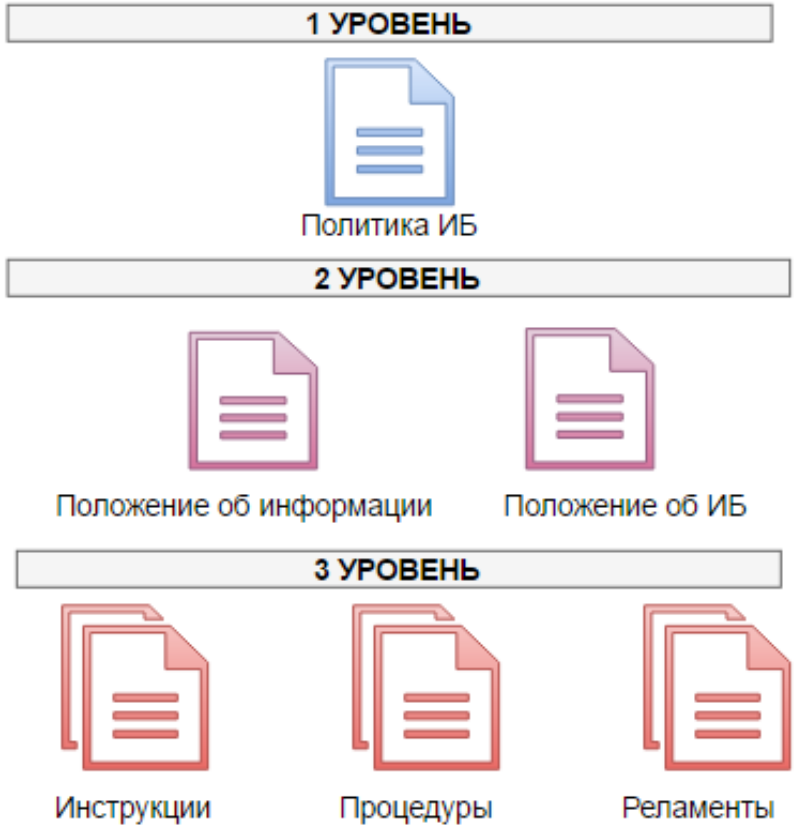

Рисунок 12 – Многоуровневая ПБ

Первый уровень носит общий характер и определяет политику организации в целом. Основное внимание уделяется: правовое обеспечение ИБ предприятия, целям, преследуемым предприятием в области информационной безопасности, целям создания политики, область действия политики.

Второй уровень политики безопасности определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией. Описывает объекты защиты, лица, ответственные за обеспечение ИБ, а также их обязанности, и ответственность за нарушение ПБ.

На третьем уровне конкретные требования, правила, инструкции по обеспечению ИБ, механизмы защиты информации и используемые программно-технические средства для их реализации.

ПБ должна соответствовать требованиям ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью, (Глава 3 – ПБ).

Международный стандарт ISO/IEC 27002 Информационные технологии. Свод правил по управлению защитой информации (Глава 5).

При внедрении ПБ предприятия можно добиться следующих целей:

– выполнение требований российского законодательства;

– выполнение требований клиентов и партнеров;

– устранение замечаний аудиторов;

– демонстрация заинтересованности руководства компании;

– создание корпоративной культуры безопасности;

– экономическая целесообразность;

– хорошая бизнес практика.

3.1 Правовая основа обеспечения ИБ предприятия

Правовой основой обеспечения ИБ являются Конституция Российской Федерации, федеральные законы, указы Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, нормативные правовые акты законодательства Российской Федерации, а также нормативные и руководящие документы ФСТЭК России и ФСБ России по вопросам защиты информации.

Основным законом в области обеспечения ИБ является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», описывающий необходимость защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации.

Деятельность предприятия регулируется федеральным закон «Об акционерных обществах» от 26.12.1995 N 208-ФЗ. В главе 13 прописаны основные требования к информации Общества, а именно о хранении документов, об обязательном раскрытии информации, и об освобождении от обязанности предоставления информации.

Защиту конфиденциальной информации, коммерческой тайны и персональных данных регулируют:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Постановление Правительства РФ от 1 ноября 2012 г. «об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

– Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ;

– Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера», постановление Правительства РСФСР от 05.12.1991 N 35 (ред. от 03.10.2002) «О перечне сведений, которые не могут составлять коммерческую тайну».

При организации электронного взаимодействия необходимо опираться на положения Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», обеспечивающего юридическую значимость электронных документов.

3.2 Цели обеспечения безопасности информации на предприятии

Главной целью обеспечения безопасности информации является предотвращение (минимизация) ущерба, в результате противоправных действий с информацией, приводящих к ее разглашению, утрате, утечке, искажению, уничтожению, незаконному использованию, нарушению функционирования предприятия.

Основными целями обеспечения безопасности информации являются:

– обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов информационных систем и сервисов;

– соблюдение правового режима обработки информации;

– предотвращение реализации угроз безопасности для деятельности на основе создания комплексной системы обеспечения информационной безопасности.

3.3 Цели и задачи создания политики безопасности

Основной целью является защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба, при случайном или преднамеренном воздействии на информацию, ее носители, процессы обработки и передачи, а также для минимизации рисков.

Данную цель можно достичь благодаря обеспечению и постоянному поддержанию основных свойств информации.

К ним относится:

– доступность информации для пользователей, т.е. постоянного функционирования информационной системы, при котором пользователи имеют возможность получения необходимой информации и результатов решения задач за приемлемое для них время;

– целостности информации, хранимой и обрабатываемой в информационной системе и передаваемой по каналам связи;

– конфиденциальности – сохранения в тайне определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи.

Необходимый уровень доступности, целостности и конфиденциальности информации должен обеспечиваться методами и средствами, в соответствии от угроз ИБ.

К основным задачам ПБ относятся:

– защита информационных активов от угроз, исходящих от противоправных действий злоумышленников,

– уменьшение рисков и снижение потенциального вреда от непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов;

– контроль целостности среды исполнения программ и ее восстановление в случае нарушения;

– защиту системы от НСД вредоносных программ;

– обеспечение работоспособности применяемых в информационных системах средств защиты информации;

– своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

– создание условий для минимизации и локализации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

3.4 Область действия ПБ

Политика безопасности распространяется на все отделы обособленного подразделения предприятия и обязательна для исполнения всеми его сотрудниками и должностными лицами.

Положения ПБ применимы для использования во внутренних нормативных и методических документах, а также в договорах.

3.5 Лица, ответственные за обеспечение ИБ

Для обеспечения ИБ, необходимо назначить лица, отвечающие за ее организацию, в виде администратора ИБ. Администратор ИБ назначается приказом генерального директора АО «Прииск Соловьевский».

На него возлагаются функции по координации действий по обеспечению достижения целей информационной безопасности.

Обязанности администратора ИБ:

– установка, сопровождение, администрирование и обеспечение функционирования средств и систем защиты информации в пределах, возложенных на него обязанностей;

– обучение персонала и пользователей ИС правилам работы со средствами защиты информации;

– определение и назначение прав пользователям ИС на доступ к защищаемым информационным;

– осуществление периодического контроля программной среды на отсутствие компьютерных вирусов;

– контроль программных средств и их целостности;

– контроль журналов регистрации событий СЗИ НСД;

– участие по согласованию с отделением технической ЗИ в проведении административных расследований фактов нарушения защищаемой информации.

3.6 Ответственность за выполнение политики безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник предприятия в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники подразделения несут персональную (в том числе материальную) ответственность за ущерб, причиненный в результате нарушения ими правил политики ИБ (ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ, уничтожение, блокирование или модификация защищаемой информации, сотрудники несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

3.7 Работа с персоналом по обеспечению ИБ

3.7.1 Определение правил и обучение им сотрудников предприятия

Руководители предприятия и сотрудники отдела, занимающегося информационной безопасностью должны уделять большое внимание отделам, в которых обрабатывается конфиденциальная информация и осуществляется доступ к защищаемым ресурсам.

Необходимо обеспечивать включение в должностные инструкции сотрудников необходимые аспекты, связанные с информационной безопасностью исполняемой должности, и контролировать их соблюдение в течение всего времени работы данного сотрудника.

В инструкциях необходимо отражать общую ответственность за проведение политики безопасности учреждения и конкретные обязанности по защите определенных ресурсов или ответственность за выполнение определенных процедур или действий по защите, связанных с исполнением должности.

При вступлении в должность нового сотрудника администратор ИБ, обязан организовать его ознакомление с инструкцией и необходимыми документами, регламентирующими требования информационной безопасности в учреждении, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем.

Сотрудников необходимо ознакомить со сведениями о политике информационной безопасности, принятых процедурах работы с информационными ресурсами, правилами доступа к информационным системам и сервисам.

Сотрудник должен быть проинформирован об угрозах нарушения режима информационной безопасности и ответственности за его нарушение. Он должен быть ознакомлен с перечнем категорированных нарушений информационной безопасности и утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников.

Также должны проверяться знания сотрудника по вопросам обеспечения информационной безопасности, требуемым на занимаемой должности, и разрешить ему допуск к исполнению должности, если его знания соответствуют установленному в учреждении уровню.

3.7.2 Правила использования рабочего стола и персонального компьютера

Правила использования рабочего стола и персонального компьютера направлены на уменьшение риска несанкционированного доступа, хищения, потери и повреждения бумажных и электронных документов и дискет в рабочее и нерабочее время.

Сотрудники обязаны выполнять следующие правила:

– бумажная документация и носители с конфиденциальной информацией, когда она не используется, должны храниться отдельно от общедоступной информации в надежных хранилищах (шкафах, сейфах), имеющих приспособления для опечатывания;

– персональные компьютеры и компьютерные терминалы, когда они не используются, необходимо защитить с помощью блокировки с ключом, паролей или других средств контроля.

– необходимо обеспечить защиту входящей и исходящей почты.

При завершении работы с информационной системой пользователи обязаны:

– завершить активные сеансы связи;

– выйти из сетевых операционных систем и сетевых сервисов по окончании сеанса связи;

– защитить ПК или терминалы с помощью блокировки с ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

3.8 Техническая безопасность

3.8.1 Политика допустимого использования

В рамках данной политики должны выполняться следующие требования:

– сотрудники несут ответственность за использование ресурсов предприятия в личных целях;

– сотрудники ответственны за безопасность паролей и учетных записей;

– при появлении у сотрудника необходимости оставить рабочее место без присмотра, все серверы, портативные компьютеры и автоматизированные рабочие места должны быть защищены паролем;

– все компьютеры, независимо от того, являются они собственностью компании или принадлежат сотруднику, должны иметь антивирусное программное обеспечение с самой последней базой обновлений;

– сотрудники должны быть внимательны при открытии вложений в сообщениях электронной почты, полученных от неизвестных отправителей;

– запрещен запуск злонамеренных программ в сети или на компьютере (например, вирусов, «червей», «Троянских коней», почтовых «бомб», и т. д.);

– запрещено разглашение собственных паролей другим сотрудникам или разрешение пользоваться кому-либо вашей учетной записью или паролями;

– запрещено использование ресурсов предприятия для создания, передачи или хранения материалов сексуального, религиозного и другого характера, не относящихся к выполнению служебных обязанностей;

– запрещены мошеннические предложения изделий, продуктов или услуг с использованием учетной записи пользователя компании;

– запрещены попытки обхода систем установления подлинности или безопасности приложений, операционных систем и оборудования.

3.8.2 Политика удаленного доступа

Цель данной политики – установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании.

Требования политики удаленного доступа:

– защищенный удаленный доступ должен строго контролироваться;

– процедура контроля должна гарантировать, что доступ к информации или сервисам получат только прошедшие проверку люди;

– сотрудник компании не должен передавать свой логин и пароль никогда и никому, включая членов семьи;

– управление удаленным доступом не должно быть сложным и приводить к возникновению ошибок;

– сотрудники компании с правами удаленного доступа должны гарантировать, что принадлежащие им или компании персональный компьютер или рабочая станция, которые удаленно подсоединены к корпоративной сети компании, не будут связаны в это же время с какой-либо другой сетью, за исключением персональных сетей, находящихся под полным контролем пользователя.

3.8.3 Требования по обеспечению антивирусной защиты

Требования к администратору ИБ для обеспечения антивирусной защиты:

− контроль и анализ еженедельных отчетов по состоянию антивирусной защиты;

− проведение периодического анализа и оценки ситуации антивирусной безопасности для контроля степени;

− проверка соблюдения порядка обновления средств и баз данных антивирусной защиты;

− осуществление контроля за состоянием средств антивирусной защиты на серверах, рабочих станциях пользователей;

− осуществление контроля за соблюдением работниками требований антивирусной защиты;

− обеспечение контроля за соблюдением требований при работе с сетью Интернет, а также за характером и объемом трафика, получаемого из сети Интернет, и его соответствия служебной необходимости;

− передача еженедельного отчета по состоянию антивирусной защиты администратору безопасности.

Требования к пользователям:

− никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя;

– удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;

– удалять спам, рекламу и другие бесполезные сообщения;

– никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;

– всегда проверять носители на наличие вирусов;

– периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

Требования к антивирусному программному обеспечению:

− применение только лицензионного антивирусного ПО;

− максимальная готовность быстрого реагирования на появление новых видов вирусных угроз;

− обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО;

− соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники;

− надежность и работоспособность антивирусного ПО в любом из предусмотренных режимов работы, по возможности, в русскоязычной среде;

− наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

3.8.4 Политика использования электронной почты

Требования данной политики:

– система электронной почты компании не должна использоваться для создания или распространения любых материалов, не связанных с деятельностью предприятия, включая материалы националистического, сексуального, порнографического, религиозного и политического характера;

– не допускается использование в личных целях. Использование ресурсов компании в личных целях приемлемо в разумных пределах, но такие электронные письма должны храниться в отдельной папке;

– запрещается отправка рекламных писем или развлекательных почтовых сообщений от имени предприятия;

– сотрудникам предприятия не следует ожидать соблюдения конфиденциальности почтовых сообщений при хранении, отсылке или приеме почты в системе электронной почты, так как компания может контролировать почтовые сообщения без уведомления сотрудника.

3.8.5 Политика использования паролей

Пользователи должны следовать установленным процедурам поддержания режима безопасности при выборе и использовании паролей.

Они обязаны выполнять следующие рекомендации:

– хранить пароли в секрете;

– не записывать пароли на бумаге, если не представляется возможным ее хранение в защищенном месте;

– изменять пароли всякий раз, когда есть указания на возможную компрометацию систем или паролей;

– выбирать пароли, содержащие не менее шести символов;

– при выборе паролей не следует использовать: месяцы года, дни недели и т.п.; фамилии, инициалы и регистрационные номера автомобилей; названия и идентификаторы структурных подразделений; номера телефонов или группы символов, состоящие из одних цифр; более двух одинаковых символов, следующих друг за другом; группы символов, состоящие из одних букв.

– изменять временные пароли при первом входе в системы;

– изменять пароли не менее одного раз в год для исключения ситуаций НСД, связанного с возможностью подбора пароля третьими лицами;

– не включать пароли в открытые сценарии автоматического входа в системы, например, в макросы или функциональные клавиши.

3.8.6 Политика использования электронной подписи

– электронный документ может быть подписан только тем закрытым ключом ЭЦП, для которого изготовлен сертификат ключа;

– риск неправомерного подписания электронного документа ЭЦП несет участник, от имени которого данный документ подписан;

– каждый участник должен иметь свой индивидуальный закрытый ключ ЭЦП для подписания исходящих от него электронных документов;

– проверка ЭЦП проводится при получении доставленного электронного документа средствами ЭЦП;

– участником используются ключи, соответствующие сертификаты ключей;

– личные ключевые носители пользователей должны храниться в сейфе;

– пересылка (передача) закрытых ключей ЭЦП по открытым каналам связи не допускается.

3.8.7 Политика резервного копирования

Требования данной политики:

– резервные копии критически важных производственных данных должны сниматься при каждом их изменении;

– необходимо иметь надлежащие средства резервного копирования;

– резервные копии должны быть надлежащим образом физически защищены;

– средства защиты носителей информации, принятые на основном рабочем месте, следует распространить на место хранения резервных копий;

– владельцы данных должны задать период сохранности критически важных производственных данных, а также требования к постоянному хранению архивных копий.

3.9 Физическая безопасность

3.9.1 Политика обеспечения безопасности серверов

Требования данной политики:

– сервера должны быть размещены в отдельном помещении, доступ в которое ограничен, либо их размещение в закрытых шкафах (стойках);

– обеспечить контроль физического доступа к серверу;

– использовать доверенные программно-аппаратные средства аутентификации и разграничения доступа;

– регулярно устанавливать обновления от производителя ОС на сервера (при каждом выходе нового обновления);

– необходимо использовать дополнительные средства очистки оперативной памяти;

– можно использовать только сервера, прошедшие проверку на отсутствие специально внедренных электронных устройств;

– сертифицированные программные средства;

– использовать антивирусные средства;

– осуществлять контроль физического доступа к серверу;

– доступ к сервисам должен журнализироваться и защищаться с использованием методов контроля доступа.

3.9.2 Политика безопасности АРМ

Требования данной политики:

– необходимо использовать автоматическое блокирование сеанса пользователя при превышении периода неактивности;

– регулярно устанавливать обновления от производителя ОС (при каждом выходе нового обновления);

– использовать системы контроля и разграничения доступа в рабочие помещения;

– принятия мер, не позволяющих применять средства удаленного наблюдения (шторы, разворот дисплея и т.п.).

– использование сертифицированных антивирусных средств и регулярного обновление баз антивирусов;

– подбор персонала, исключающего возможность сговора для проведения деструктивных действий;

– выполнение регламента по резервному копированию информации.

3.10 Порядок утверждения, внесения изменений и дополнений.

Настоящая Политика ИБ вступает в силу с даты утверждения.

В случае вступления отдельных пунктов в противоречие с новыми законодательными актами, эти пункты утрачивают юридическую силу до момента внесения изменений в настоящую Политику ИБ.

Пересмотр Политики информационной безопасности производится не реже одного раза в год и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

Безопасность жизнедеятельности (БЖД) – это совокупность действий, направленных на безопасное взаимодействие человека со средой обитания и его защиту, а именно, разработку методов и средств защиты, которые достигаются благодаря снижению влияния вредных и опасных факторов до допустимых значений, а также разработку мер по минимизации ущерба в ликвидации последствий ЧС мирного и военного времени.

Цели БЖД в обособленном подразделении АО «Прииск Соловьевский»:

– описание и изучение факторов окружающей среды, отрицательно влияющих на здоровье сотрудника;

– минимизация действия этих факторов до безопасных пределов или их исключение;

– установление оптимальных соотношений между факторами производственной среды для снижения неблагоприятного воздействия производственных факторов на работника;

– обеспечение безопасности выполнения работ.

Данный раздел выпускной работы посвящен определению оптимальных условий труда работников предприятия, рассмотрению уровня освещенности и уровня шума.

4.1 Безопасность жизнедеятельности пользователя ПК

Согласно статье 212 Трудового Кодекса законодательство определяет право работника на безопасные условия труда. Рабочее место – это совокупность факторов окружающей среды, в том числе и вредных.

Вредный производственный фактор негативно влияет на работника, в некоторых случаях, приводит к заболеванию или снижению работоспособности. Вредный производственный фактор, в зависимости от интенсивности и продолжительности воздействия, может стать опасным. Опасный производственный фактор в определённых условиях, приводит к травмам или ухудшению здоровья.

К вредным и опасным производственным факторам относятся:

– повышенный уровень шума (источники: вентиляционные устройства ЭВМ, устройства ввода-вывода, агрегаты кондиционирования и вентилирования воздуха, другие электрические приборы);

– высокие уровни электростатического и электромагнитного излучения, (источники: видеотерминалы);

– плохой микроклимат помещения (повышенная и пониженная температура воздуха, чрезмерная запыленность и загазованность воздуха, повышенная и пониженная влажность воздуха);

– недостаточная освещенность рабочего места;

– опасность поражения электрическим током;

– блеклость экрана дисплея;

– нарушение эргономических норм при работе с компьютером.

4.1.1 Микроклимат рабочей зоны

Микроклимат рабочего помещения – это климат внутренней среды данного помещения, который определяется показаниями температуры, влажности и скорости движения воздуха.

Средняя температура воздуха в помещении офиса должна составлять +22°С, относительная влажность – 46%, атмосферное давление – 750 мм.рт.ст., содержание пыли – не более 10 мг/м воздуха рабочего места, максимальные размеры частиц – 2 мкм. Для поддержания нормального микроклимата необходимо обеспечить достаточный объем вентиляции. Для этого в помещении должны быть предусмотрены системы отопления, вентиляции и кондиционирования.

Для повышения влажности воздуха в помещении должны применяться увлажнители воздуха с дистиллированной или кипяченой питьевой водой.

4.1.2 Освещение рабочего места

Работа, выполняемая с использованием вычислительной техники, имеют следующие недостатки:

– ухудшенная контрастность между изображением и фоном;

– отражение экрана.

При выполнении зрительных работ высокой точности общая освещенность должна составлять 300 лк, а комбинированная – 750 лк; аналогичные требования при выполнении работ средней точности – 200 и 300 лк соответственно. При этом монитор и источники света должны быть расположены, не создавая бликов на поверхности экрана. Также необходимо чтобы освещение было равномерным. Степень освещения помещения и яркость экрана компьютера должны быть примерно одинаковыми, в связи с тем, что яркий свет в районе периферийного зрения значительно увеличивает напряженность глаз и приводит к их быстрой утомляемости.

Рабочее место с ЭВМ должны иметь естественное и искусственное освещение. Дополнительное искусственное освещение должно применяться не только в темное, но и в светлое время суток. Естественное освещение должно осуществляться через световые проемы, ориентированные преимущественно на север и северо-восток и обеспечивать коэффициенты естественной освещенности (КЕО) не ниже 1.2% в зонах с устойчивым снежным покровом и 1.5% на остальной территории. Искусственное освещение в помещениях эксплуатации ЭВМ должно осуществляться системой общего равномерного освещения. Источниками искусственного освещения могут быть люминесцентные лампы типа ЛБ или ДРЛ, которые попарно объединяются в светильники, расположенные над рабочими поверхностями равномерно.

Рабочие места, работающих с дисплеями, располагают подальше от окон и таким образом, чтобы оконные проемы находились сбоку от них. Окна в помещениях должны быть ориентированы на север и северо-восток. Оконные проемы должны быть оснащены регулируемыми устройствами типа: светорассеивающих штор, регулируемыми жалюзи или солнцезащитной пленкой с металлическим покрытием, занавесей, внешних козырьков и др.

4.1.3 Шум и вибрация

Шум ухудшает условия труда, оказывая вредное действие на организм человека. Последствиями шумового воздействия являются раздражительность, головные боли, головокружение, снижение памяти, повышенную утомляемость,

понижение аппетита, боли в ушах и т. д. Все это может вызвать негативные изменения в эмоциональном состоянии человека вплоть до стрессовых. Также снижается концентрация внимания, нарушаются физиологические функции, появляется, ухудшается речевая коммутация. Все это снижает работоспособность человека и его производительность, качество и безопасность труда. Длительное воздействие интенсивного шума (выше 80 дБ) на слух человека приводит к его частичной или полной потере.

Уровень шума на рабочем месте математиков-программистов и операторов видеоматериалов не должен превышать 50 дБ, а в залах обработки информации на вычислительных машинах – 65 дБ. Для снижения уровня шума стены и потолок помещений, могут быть облицованы звукопоглощающими материалами. Уровень вибрации в помещениях вычислительных центров может быть снижен путем установки оборудования на специальные виброизоляторы.

4.1.4 Воздействие электромагнитных излучений

При эксплуатации монитор компьютера излучает мягкое рентгеновское излучение. Этот вид излучения опасен тем, что может проникать в тело человека на глубину 1-2 см и поражать поверхностный кожный покров.

Максимальный уровень рентгеновского излучения на рабочем месте программиста обычно не превышает 10 мкбэр/ч, а интенсивность ультрафиолетового и инфракрасного излучений от экрана монитора лежит в пределах 10-100мВт/м2.

Ультрафиолетовое излучение в больших дозах может вызвать дерматит кожи, головную боль, резь в глазах.

Инфракрасное излучение приводит к перегреву тканей человека (особенно хрусталика глаза), повышению температуры тела.

Уровни напряженности электростатических полей должны составлять не более 20 кВ/м. Поверхностный электростатический потенциал не должен превышать 500 В. При повышенном уровне напряженности полей следует сократить время работы за компьютером, делать пятнадцатиминутные перерывы в течение

полутора часов работы, обязательно применять защитные экраны, не размещать их концентрированно в рабочей зоне и выключать их, если на них не работают.

Электробезопасность в рабочем помещении обеспечивается техническими способами и средствами защиты, а также организационными и техническими мероприятиями.

В течение работы на корпусе компьютера накапливается статическое электричество. На расстоянии 5 – 10 см от экрана напряженность электростатического поля составляет 60 – 280 кВ/м, то есть в 10 раз превышает норму 20 кВ/м. Для уменьшения напряжённости применять применение увлажнители и нейтрализаторы, антистатическое покрытия пола.

Для обеспечения защиты от поражения электрическим током при прикосновении к металлическим нетоковедущим частям, которые могут оказаться под напряжением в результате повреждения изоляции, я рекомендую применять защитное заземление.

Заземление корпуса ЭВМ обеспечено подведением заземляющей жилы к питающим розеткам. Сопротивление заземления 4 Ом, согласно (ПУЭ) для электроустановок с напряжением до 1000 В.

Также необходимо проводить организационные мероприятия, а именно, инструктаж и обучение безопасным методам труда, а также проверка знаний правил безопасности и инструкций в соответствии с занимаемой должностью применительно к выполняемой работе.

4.2 Экологичность

Макулатура является самым распространенным канцелярским предметом в офисах и учебных заведениях. ГОСТ Р 55090-2012 дает рекомендации по утилизации макулатуры.

К основным мероприятиям по регулированию в области обращения с отходами и утилизации макулатуры относят:

– основной принцип – загрязнитель платит;

– обеспечение производителями и потребителями эффективных мер для надлежащего использования расходов необходимых для предотвращения неблагоприятного экологического воздействия при производстве бумаги и утилизации макулатуры;

– осуществление политики комплексного управления отходами, разработка и реализация мер, направленных на уменьшение образования отходов и содействие их переработке, при условии обеспечения мер, не допускающих диспропорции в международной торговле;

– стимулирование роста переработки большей части макулатуры, которая составляет значительную долю (от 25 до 50 процентов) твердых бытовых отходов, в бумажную продукцию с учетом того, что производство бумаги и картона с использованием переработанных волокон, как правило, является менее энергозатратным и более чистым с экологической точки зрения чем аналогичное производство посредством переработки целлюлозы;

– организация и финансирование исследований в области разработок более выгодных технологий использования макулатуры, чем производство бумаги и картона;

– принятие экономических мер с учетом того, что экономика отрасли по переработке макулатуры для производства бумаги и картона характеризуется значительными колебаниями цен на макулатуру;

– принятие мер по снижению высоких затрат на сбор и сортировку отходов для снижения затрат на переработку макулатуры;

– проведение экономического анализа процессов утилизации для осуществления экономии затрат на утилизацию отходов; анализ и внедрение практических мер, направленных на увеличение спроса, как на переработанную макулатуру, так и на поставку вторичных волокон.

4.3 Чрезвычайные ситуации

Для снижения или предотвращения влияния опасных и вредных факторов необходимо соблюдать санитарные правила и нормы. гигиенические требования к видео-дисплейным терминалам, персональным электронно-вычислительным

машинам и организации работы (Утверждено Постановлением Госкомсанэпиднадзора России от 14 июля 1996 г. N 14 СанПиН 2.2.2.542-96), и Приложение 1,2

Во избежание повреждения изоляции проводов и возникновения коротких замыканий не разрешается: вешать что-либо на провода, закрашивать и белить шнуры и провода, закладывать провода и шнуры за газовые и водопроводные трубы, за батареи отопительной системы, выдергивать штепсельную вилку из розетки за шнур, усилие должно быть приложено к корпусу вилки.

Для исключения поражения электрическим током запрещается: часто включать и выключать компьютер без необходимости, прикасаться к экрану и к тыльной стороне блоков компьютера, работать на средствах вычислительной техники и периферийном оборудовании мокрыми руками, работать на средствах вычислительной техники и периферийном оборудовании, имеющих нарушения целостности корпуса, нарушения изоляции проводов, неисправную индикацию включения питания, с признаками электрического напряжения на корпусе, класть на средства вычислительной техники и периферийном оборудовании посторонние предметы.

Запрещается под напряжением очищать от пыли и загрязнения электрооборудование.

Запрещается проверять работоспособность электрооборудования в неприспособленных для эксплуатации помещениях с токопроводящими полами, сырых, не позволяющих заземлить доступные металлические части.

Недопустимо под напряжением проводить ремонт средств вычислительной техники и периферийного оборудования. Ремонт электроаппаратуры производится только специалистами-техниками с соблюдением необходимых технических требований.

ЗАКЛЮЧЕНИЕ

Произведенные работы в ходе выполнения выпускной квалификационной работы позволили выполнить поставленную цель, а именно разработать политику информационной безопасности обособленного подразделения предприятия АО «Прииск Соловьевский».

Для достижения поставленной цели были выполнены следующие задачи:

− проанализирована система информационной безопасности предприятия;

− идентифицированы и оценены информационные активы предприятия;

− произведена оценка угроз и соответствующим им уязвимостей;

− описаны средства защиты, использующиеся на предприятии;

− оценены риски активов;

− даны рекомендации по обеспечению физической, аппаратно-технической и программной безопасности;

− представлены средства для их реализации;

− дано экономическое обоснование выбранных мер;

− описана безопасность жизнедеятельности на предприятии.

В совокупности были выполнены все поставленные для данной выпускной квалификационной работы задачи.

БИБИЛИОГРАФИЧЕСКИЙ СПИСОК

1 Астахова, Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций/ Л.В.Астахова. – Челябинск: Изд-во «ЗАО Челябинская межрайонная типография», 2006г. – 361 с.

2 Бабаш, А.В. Информационная безопасность. Лабораторный практикум: Учебное пособие / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников. – М.: КноРус, 2013. – 136 с.

3 ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – М.: Изд-во стандартов, 2006. – 12 с.

4 ГОСТ Р 50922–2006. Защита информации. Основные термины и определения. – Взамен ГОСТ Р 50922–96; введ. 2006–01–01. – М.: Изд-во стандартов, 2008. – 27 с.

5 ГОСТ Р 51275—2006. Защита информации. Объект информации. Факторы, воздействующие на информацию. Общие положения. – Взамен ГОСТ Р 51275–99; введ. 2008-02-01 – М.: Изд-во стандартов, 2007. – 11 с.

6 ГОСТ Р ИСО 6385–2016. Эргономика. Применение эргономических принципов при проектировании производственных систем. – Взамен ГОСТ ГОСТ Р ИСО 6385–2007;введ. 2017–12–01. – М.: Изд-во стандартов, 2016. – 20 с.

7 ГОСТ Р ИСО/МЭК 15408–1–2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. – Взамен ГОСТ Р ИСО/МЭК 15408–1–2002; введ. 2009-10-01. – М.: Изд-во стандартов, 2009. – 40 с.

8 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – М.: Изд-во стандартов, 2014. – 104 с.

9 ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности. – Взамен ГОСТ Р ИСО/МЭК 17799-2005; введ. 2014–01–01. – М.: Изд-во стандартов, 2014. – 104с.

10 Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. - Ст. Оскол: ТНТ, 2010. –384 с.

11 Качановский, Ю.П. Основные технические, программные и организационные меры защиты информации при работе с компьютерными системами [Электронный ресурс]: методические указания к проведению лабораторной работы по курсу «Информатика»/ Ю.П. Качановский, А.С. Широков – Электрон. текстовые данные.– Липецк: Липецкий государственный технический университет, 2014. – 24 с. – Режим доступа: http://www.iprbookshop.ru/55120.html. – ЭБС «IPRbooks»

12 Методические указания по выполнению курсовой работы по дисциплине «Организационные меры защиты систем» для студентов направления подготовки 09.03.02 Информационные системы и технологии / С.Г. Самохвалова – Благовещенск: ФГБОУ ВО «АмГУ», 2017 г. – 30 с.

13 Петренко, С.А. Политики безопасности компании при работе в Интернет [Электронный ресурс]/ Петренко С.А., Курбатов В.А. – Электрон. текстовые данные. – М.: ДМК Пресс, 2011. – 400 с. ресурс] : офиц. сайт. – 2003 – Режим доступа:http://bookz.ru/authors/sergei-petrenko/politiki_424/– 25.05.2017

14 Плахов, А.М. Безопасность жизнедеятельности: Учебное пособие/ А.М.Плахов. – Томск: Изд-во ТПУ, 2006. – 180 с.

15 Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Приказ ФСТЭК от 30 марта 1992 г. – 1992. – 29 с.

16 Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. – Приказ ФСТЭК от 30 марта 1992 г. – 1992. 29 с.

17 Шаньгин В.Ф. Информационная безопасность и защита информации [Электронный ресурс] / В.Ф. Шаньгин – Электрон. текстовые данные. – Саратов:

Профобразование, 2017. – 702 с. – Режим доступа: http://www.iprbookshop.ru/ – ЭБС «IPRbooks»

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

ПРИЛОЖЕНИЕ А

Схема линейной организационной структуры

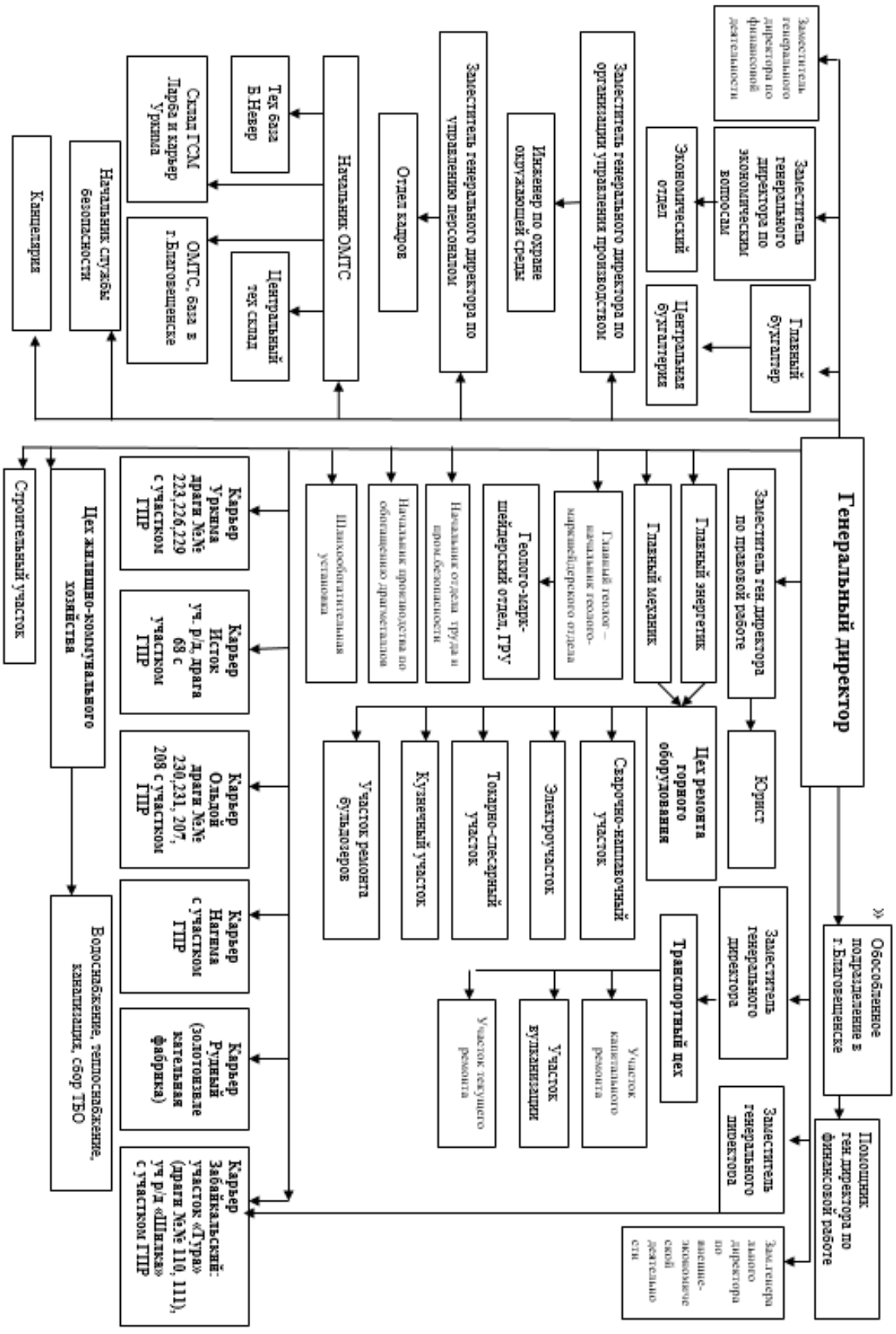

Рисунок А.1 – Организационная структура предприятия

ПРИЛОЖЕНИЕ Б

Схемы потоков данных

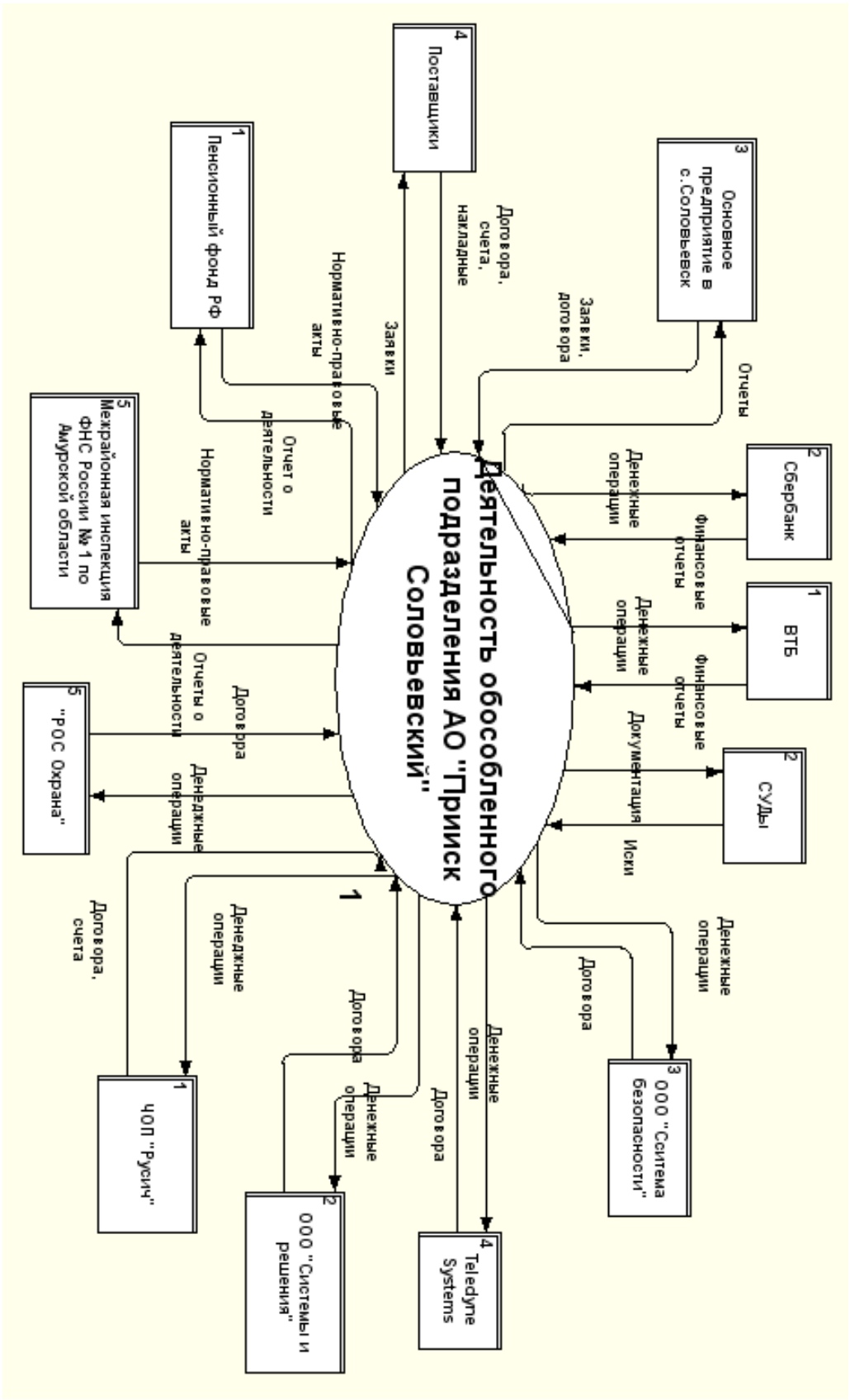

Рисунок Б.1 – Внешний документооборот

Продолжение ПРИЛОЖЕНИЯ Б

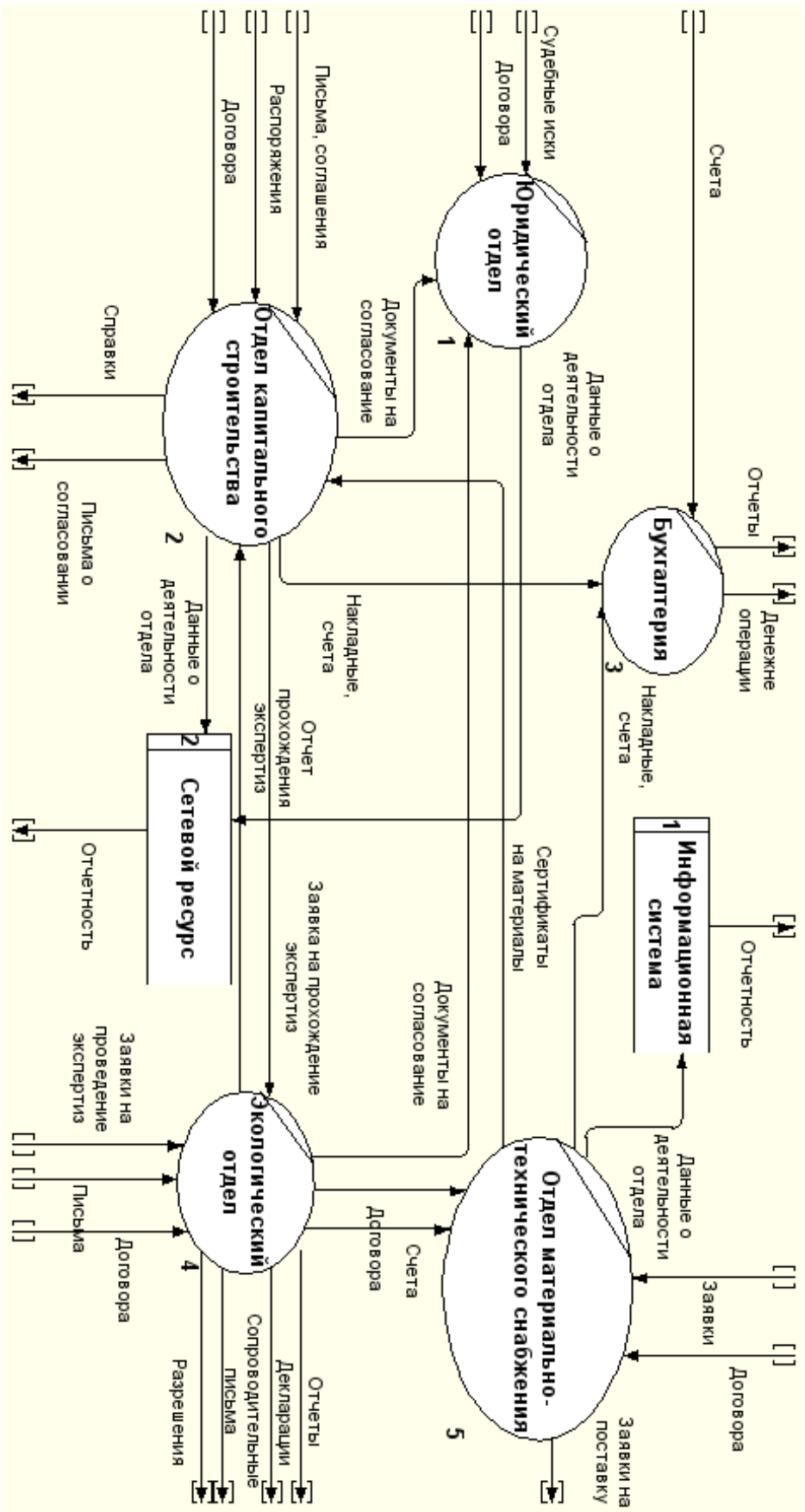

Рисунок Б.2 – Внутренний документооборот

ПРИЛОЖЕНИЕ В

Политика информационной безопасности АО «Прииск Соловьевский»

Содержание

1 Общие положения

1.1 Настоящая Политика разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения информационной безопасности

1.2 Настоящая Политика является документом, доступным любому сотруднику предприятия и пользователю его ресурсов, и представляет собой систему взглядов на проблему обеспечения информационной безопасности, и устанавливает принципы построения системы управления информационной безопасностью на основе изложения целей, процессов и процедур информационной безопасности

1.3 Настоящая Политика распространяется всех сотрудников и руководство, а также пользователей его информационных ресурсов.

2 Обозначения и сокращения

АРМ – Автоматизированное рабочее место.
АС – Автоматизированная система.
ЭЦП – Электронно-цифровая подпись.
ЗИ – Защита информации.
ИБ – Информационная безопасность.

ИС – Информационная система.
ИТС – Информационно-телекоммуникационная система.
НСД – Несанкционированный доступ.
ОС – Операционная система.
ПБ – Политики безопасности.
ПО – Программное обеспечение.
СВТ – Средства вычислительной техники.
СЗИ – Средство защиты информации.
СПД – Система передачи данных.
СУИБ – Система управления информационной безопасностью.
ЭВМ – Электронная - вычислительная машина.
ЭЦП – Электронная цифровая подпись.
МЭ – Межсетевой экран.

3 Правовая основа обеспечения ИБ предприятия

Правовой основой обеспечения ИБ являются Конституция Российской Федерации, федеральные законы, указы Президента Российской Федерации, постановления и распоряжения Правительства Российской Федерации, нормативные правовые акты законодательства Российской Федерации, а также нормативные и руководящие документы ФСТЭК России и ФСБ России по вопросам защиты информации.

Основным законом в области обеспечения ИБ является Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации», описывающий необходимость защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении информации.

Деятельность предприятия регулируется федеральным закон «Об акционерных обществах» от 26.12.1995 N 208-ФЗ. В главе 13 прописаны основные требования к информации Общества, а именно о хранении документов, об обязательном раскрытии информации, и об освобождении от обязанности предоставления информации.

Защиту конфиденциальной информации, коммерческой тайны и персональных данных регулируют:

– Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;

– Постановление Правительства РФ от 1 ноября 2012 г. n 1119 “об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных”;

– Федеральный закон «О коммерческой тайне» от 29.07.2004 N 98-ФЗ;

– Указ Президента РФ от 06.03.1997 N 188 (ред. от 13.07.2015) «Об утверждении перечня сведений конфиденциального характера»;

− Постановление Правительства РСФСР от 05.12.1991 N 35 (ред. от 03.10.2002) «О перечне сведений, которые не могут составлять коммерческую тайну»;

– при организации электронного взаимодействия необходимо опираться на положения Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», обеспечивающего юридическую значимость электронных документов.

4 Цели обеспечения безопасности информации на предприятии

Главной целью обеспечения безопасности информации является предотвращение (минимизация) ущерба, в результате противоправных действий с информацией, приводящих к ее разглашению, утрате, утечке, искажению, уничтожению или незаконному использованию, либо нарушению функционирования предприятия.

Основными целями обеспечения безопасности информации являются:

– обеспечение устойчивого и корректного функционирования программных и аппаратных компонентов информационных систем и сервисов;

– соблюдение правового режима использования массивов и программ обработки информации;

– предотвращение реализации угроз безопасности для деятельности на основе создания комплексной системы обеспечения информационной безопасности.

5 Цели и задачи создания политики безопасности

Основной целью настоящей Политики является защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба, при случайном или преднамеренном воздействии на информацию, ее носители, процессы обработки и передачи, а также для минимизации рисков.

Данную цель можно достичь благодаря обеспечению и постоянному поддержанию основных свойств информации: конфиденциальности, целостности и доступности.

К основным задачам ПБ относятся:

– защита информационных активов от угроз, исходящих от противоправных действий злоумышленников;

– уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации;

– контроль целостности среды исполнения программ и ее восстановление в случае нарушения;

– защиту системы от несанкционированного внедрения вредоносных программ, включая компьютерные вирусы;

– защиту информации ограниченного распространения;

– обеспечение работоспособности применяемых в информационных системах средств защиты информации;

– своевременное выявление источников угроз безопасности информации, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;

6 Область действия ПБ

Политика безопасности распространяется на все отделы обособленного подразделения предприятия и обязательна для исполнения всеми его сотрудниками и должностными лицами.

Положения ПБ применимы для использования во внутренних нормативных и методических документах, а также в договорах.

7 Лица, ответственные за обеспечение ИБ

Для обеспечения ИБ, необходимо назначить лица, отвечающие за ее организацию, в виде администратора ИБ. Администратор ИБ назначается приказом Генеральный директора АО «Прииск Соловьевский».

На него возлагаются функции по координации действий по обеспечению достижения целей информационной безопасности.

Обязанности администратора ИБ:

– установка, сопровождение, администрирование и обеспечение функционирования средств и систем защиты информации в пределах, возложенных на него обязанностей;

– обучение персонала и пользователей ИС правилам работы со средствами защиты информации;

– определение и назначение прав пользователям ИС на доступ к защищаемым информационным;

– осуществление периодического контроля программной среды на отсутствие компьютерных вирусов;

– контроль журналов регистрации событий СЗИ НСД;

– участие по согласованию с отделением технической защиты информации в проведении административных расследований фактов нарушения или угрозы нарушения безопасности защищаемой информации.

8 Ответственность за выполнение политики безопасности

Ответственность за выполнение правил ПБ несет каждый сотрудник предприятия в рамках своих служебных обязанностей и полномочий.

На основании ст. 192 Трудового кодекса РФ сотрудники, нарушающие требования политики безопасности, могут быть подвергнуты дисциплинарным взысканиям, включая замечание, выговор и увольнение с работы.

Все сотрудники несут персональную (в том числе материальную) ответственность за прямой действительный ущерб, причиненный Организации в результате нарушения ими правил политики ИБ (ст. 238 Трудового кодекса РФ).

За неправомерный доступ к компьютерной информации, создание, использование или распространение вредоносных программ, а также нарушение правил эксплуатации ЭВМ, следствием которых явилось нарушение работы ЭВМ, уничтожение, блокирование или модификация защищаемой информации, сотрудники несут ответственность в соответствии со статьями 272, 273 и 274 Уголовного кодекса Российской Федерации.

9 Объект защиты

К информационным объектам защиты относятся: бумажные носители, информация в электронном виде, цифровые сигналы, аналоговые сигналы.

К ресурсным: аппаратное обеспечение, программное обеспечение, процессы обработки информации, сервера.

К физическим: здание, помещение, территория, техническое оборудование, сетевые каналы, каналы связи.

К пользовательским: персонал, пользователи информации, собственники информации, обслуживающий персонал.

Процессами, подлежащими защите можно обозначить всю деятельность обособленного подразделения, связанную со сбором, обработкой, систематизацией, накоплением, уточнением, использованием, хранением, уничтожением и передачей конфиденциальной информации.

Защите подлежит вся информация и информационные ресурсы предприятия, независимо от их формы представления и местоположения в информационной системе подразделения.

10 Работа с персоналом по обеспечению ИБ

10.1 Определение правил и обучение им сотрудников предприятия

Руководители предприятия и сотрудники отдела, занимающегося информационной безопасностью должны уделять большое внимание отделам, в которых обрабатывается конфиденциальная информация и осуществляется доступ к защищаемым ресурсам.

Необходимо обеспечивать включение в должностные инструкции сотрудников необходимые аспекты, связанные с информационной безопасностью исполняемой должности, и контролировать их соблюдение в течение всего времени работы данного сотрудника.

В инструкциях необходимо отражать общую ответственность за проведение политики безопасности учреждения и конкретные обязанности по защите определенных ресурсов или ответственность за выполнение определенных процедур или действий по защите, связанных с исполнением должности.

При вступлении в должность нового сотрудника администратор ИБ, обязан организовать его ознакомление с инструкцией и необходимыми документами, регламентирующими требования информационной безопасности в учреждении, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем.

Сотрудников необходимо ознакомить со сведениями о политике информационной безопасности, принятых процедурах работы с документами и информационными ресурсами, правилами доступа к информационным системам и сервисам, а также, в письменной форме предоставить, разрешенный ему доступ (права и ограничения) к информационным ресурсам.

Сотрудник должен быть ознакомлен с перечнем категорированных нарушений информационной безопасности и утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые в учреждении политику и процедуры безопасности.

Также должны проверяться знания сотрудника по вопросам обеспечения информационной безопасности, требуемым на занимаемой должности, и разрешить ему допуск к исполнению должности, если его знания соответствуют установленному в учреждении уровню.

10.2 Правила использования рабочего стола и персонального компьютера

Для обеспечения установленного режима информационной безопасности в учреждении определяются правила использования рабочего стола и персонального компьютера, которые направлены на уменьшение риска несанкционированного доступа, хищения, потери и повреждения бумажных и электронных документов и дискет в рабочее и нерабочее время.

Сотрудники учреждения обязаны выполнять следующие рекомендации:

– бумажная документация и носители с конфиденциальной информацией, когда она не используется, должны храниться отдельно от общедоступной информации в надежных хранилищах (шкафах, сейфах), имеющих приспособления для опечатывания;

– персональные компьютеры и компьютерные терминалы, когда они не используются, необходимо защитить с помощью блокировки с ключом, паролей или других средств контроля;

– необходимо обеспечить защиту входящей и исходящей почты.

11 Техническая безопасность

11.1 Политика допустимого использования

В рамках данной политики должны выполняться следующие требования:

– сотрудники несут ответственность за использование ресурсов предприятия в личных целях;

– сотрудники ответственны за безопасность их паролей и учетных записей;

– при появлении у сотрудника необходимости оставить рабочее место без присмотра, все серверы, портативные компьютеры и автоматизированные рабочие места должны быть защищены паролем;

– все компьютеры, используемые сотрудниками для доступа к ресурсам компании, независимо от того, являются они собственностью компании или принадлежат сотруднику, должны иметь антивирусное программное обеспечение с самой последней базой обновлений;

– сотрудники должны быть внимательны при открытии вложений в сообщениях электронной почты, полученных от неизвестных отправителей;

– запрещен запуск злонамеренных программ в сети или на компьютере (например, вирусов, «червей», «Троянских коней», почтовых «бомб», и т. д.);

– запрещено разглашение собственных паролей другим сотрудникам или разрешение пользоваться кому-либо вашей учетной записью или паролями;

– запрещено использование ресурсов предприятия для создания, передачи или хранения материалов сексуального, религиозного и другого характера, не относящихся к выполнению служебных обязанностей;

– запрещены мошеннические предложения изделий, продуктов или услуг с использованием учетной записи пользователя компании;

– запрещены попытки обхода систем установления подлинности или безопасности приложений, операционных систем и оборудования.

11.2 Политика удаленного доступа

Цель данной политики - установление стандартных норм безопасного удаленного соединения любого хоста с сетью компании.

Требования политики удаленного доступа:

– защищенный удаленный доступ должен строго контролироваться;

– процедура контроля должна гарантировать, что доступ к информации или сервисам получат только прошедшие проверку люди;

– сотрудник компании не должен передавать свой логин и пароль никогда и никому, включая членов семьи;

– управление удаленным доступом не должно быть сложным и приводить к возникновению ошибок;

– сотрудники компании с правами удаленного доступа должны гарантировать, что принадлежащие им или компании персональный компьютер или рабочая станция, которые удаленно подсоединены к корпоративной сети компании, не будут связаны в это же время с какой-либо другой сетью, за исключением персональных сетей, находящихся под полным контролем пользователя.

11.3 Требования по обеспечению антивирусной защиты

Требования к администратору ИБ для обеспечения антивирусной защиты:

− контроль и анализ еженедельных отчетов по состоянию антивирусной защиты;

− проведение периодического анализа и оценки ситуации антивирусной безопасности для контроля степени;

− проверка соблюдения порядка обновления средств и баз данных антивирусной защиты;

− осуществление контроля за состоянием средств антивирусной защиты на серверах, рабочих станциях пользователей;

− осуществление контроля за соблюдением работниками требований антивирусной защиты;

− передача еженедельного отчета по состоянию антивирусной защиты администратору безопасности.

Требования к пользователям:

− никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя;

– удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;

– удалять спам, рекламу и другие бесполезные сообщения;

– никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;

– всегда проверять носители на наличие вирусов;

– периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

Требования к антивирусному программному обеспечению:

− применение только лицензионного антивирусного ПО;

− максимальная готовность быстрого реагирования на появление новых видов вирусных угроз;

− обеспечение обновлений, консультаций и других форм сопровождения эксплуатации поставщиком антивирусного ПО;

− соответствие системных требований антивирусного ПО платформам, характеристикам и комплектации применяемой вычислительной техники;

− наличие документации, необходимой для практического применения и освоения антивирусного ПО, на русском языке.

11.4 Политика использования электронной почты

Требования данной политики:

– система электронной почты компании не должна использоваться для создания или распространения любых материалов, не связанных с деятельностью предприятия, включая материалы националистического, сексуального, порнографического, религиозного и политического характера;

– не допускается использование в личных целях. Использование ресурсов компании в личных целях приемлемо в разумных пределах, но такие электронные письма должны храниться в отдельной папке;

Запрещается отправка рекламных писем или развлекательных почтовых сообщений от имени компании запрещена;

– сотрудникам предприятия не следует ожидать соблюдения конфиденциальности почтовых сообщений при хранении, отсылке или приеме почты в системе электронной почты, так как компания может контролировать почтовые сообщения без уведомления сотрудника.

11.5 Политика использования паролей

Пользователи должны следовать установленным процедурам поддержания режима безопасности при выборе и использовании паролей. Они обязаны выполнять следующие рекомендации:

– хранить пароли в секрете;

– не записывать пароли на бумаге, если не представляется возможным ее хранение в защищенном месте;

– изменять пароли всякий раз, когда есть указания на возможную компрометацию систем или паролей;

– выбирать пароли, содержащие не менее шести символов;

– при выборе паролей не следует использовать: месяцы года, дни недели и т.п.; фамилии, инициалы и регистрационные номера автомобилей; названия и идентификаторы структурных подразделений; номера телефонов или группы символов, состоящие из одних цифр; пользовательские идентификаторы и имена, а также идентификаторы групп и другие системные идентификаторы; более двух одинаковых символов, следующих друг за другом; группы символов, состоящие из одних букв.

– изменять временные пароли при первом входе в системы;

– изменять пароли не менее одного раз в год для исключения ситуаций несанкционированного доступа, связанного с возможностью подбора пароля третьими лицами;

– не включать пароли в открытые сценарии автоматического входа в системы, например, в макросы или функциональные клавиши.

11.6 Политика использования электронной подписи.

– электронный документ может быть подписан только тем закрытым ключом ЭЦП, для которого изготовлен сертификат ключа;

– электронный документ считается исходящим от участника, если он подписан ЭЦП, владельцем сертификата ключа которой является данный участник;

– риск неправомерного подписания электронного документа ЭЦП несет участник, от имени которого данный документ подписан;

– каждый участник должен иметь свой индивидуальный закрытый ключ ЭЦП для подписания исходящих от него электронных документов;

– проверка ЭЦП проводится при получении доставленного электронного документа средствами ЭЦП;

– участником используются ключи, соответствующие сертификаты ключей;

– личные ключевые носители пользователей должны храниться в сейфе;

– ответственность за конфиденциальность пароля возлагается на владельца закрытого ключа;

– пересылка (передача) закрытых ключей ЭЦП по открытым каналам связи не допускается;

– в целях обеспечения конфиденциальности ключей, вышедших из обращения, может применяться процедура уничтожения с использованием средств ЭЦП.

11.7 Политика резервного копирования

Требования данной политики:

– резервные копии критически важных производственных данных должны сниматься при каждом их изменении;

– для обеспечения возможности восстановления всех критически важных производственных данных и программ после выхода из строя компьютера или отказа носителя информации, необходимо иметь надлежащие средства резервного копирования;

– резервные копии должны быть надлежащим образом физически защищены;

– владельцы данных должны задать период сохранности критически важных производственных данных, а также требования к постоянному хранению архивных копий.

12 Физическая безопасность

12.1 Политика обеспечения безопасности серверов

Требования данной политики:

– сервера должны быть размещены в отдельном помещении, доступ в которое ограничен, либо их размещение в закрытых шкафах (стойках);

– обеспечить контроль физического доступа к серверу:

– использовать доверенные программно-аппаратные средства аутентификации и разграничения доступа;

– регулярно устанавливать обновления от производителя ОС на сервера (при каждом выходе нового обновления);

– необходимо использовать дополнительные средства очистки оперативной памяти;

– можно использовать только сервера, прошедшие проверку на отсутствие специально внедренных электронных устройств;

– сертифицированные программные средства;

– использовать антивирусные средства;

– осуществлять контроль физического доступа к серверу;

–

– доступ к сервисам должен журнализироваться и защищаться с использованием методов контроля доступа.

12.2 Политика безопасности АРМ

– необходимо использовать автоматическое блокирование сеанса пользователя при превышении периода неактивности;

– регулярно устанавливать обновления от производителя ОС (при каждом выходе нового обновления);

– использовать системы контроля и разграничения доступа в рабочие помещения;

− принятия мер, не позволяющих применять средства удаленного наблюдения (шторы, разворот дисплея и т.п.).

– Использование сертифицированных антивирусных средств и регулярного обновление баз антивирусов;

– Подбор персонала, исключающего возможность сговора для проведения деструктивных действий;

– Выполнение регламента по резервному копированию информации.

13 Порядок утверждения, внесения изменений и дополнений.

Настоящая Политика ИБ вступает в силу с даты утверждения.

В случае вступления отдельных пунктов в противоречие с новыми законодательными актами, эти пункты утрачивают юридическую силу до момента внесения изменений в настоящую Политику ИБ.

Пересмотр Политики информационной безопасности производится не реже одного раза в год и имеет целью приведение в соответствие определенных Политикой защитных мер реальным условиям и текущим требованиям к защите информации.

ПРИЛОЖЕНИЕ Г

Техническое задание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование системы

Полное наименование разрабатываемой информационной системы: Анализ и разработка рекомендаций по обеспечению информационной безопасности обособленного подразделения АО «Прииск Соловьевский» в г. Благовещенске

1.2 Наименование предприятий (объединений) разработчика и заказчика (пользователя) системы и их реквизиты

Разработчик: Нечипоренко Анна Сергеевна

Реквизиты разработчика:

Название учреждения разработчика: ФГБОУ ВО «АмГУ»

Юридический Адрес разработчика: 675027, Амурская область, г. Благовещенск, Игнатьевское шоссе, 21.

Телефон разработчика: 8(996)383-80-28.

E-mail разработчика: www.anna2911@mail.ru

Заказчик: АО «Прииск Соловьевский»

Реквизиты заказчика:

ИНН 2828002272

ОГРН 22193264

Название учреждения заказчика: Акционерное общество «Прииск Соловьеский»

Юридический Адрес заказчика: 676271, Амурская область, Тындинский район, с. Соловьевск, ул. Советская, д. 47

Офис заказчика: 675000 Амурская область, г. Благовещенск, ул. Зейская 259.

Телефон заказчика: (416) 5634415; (41656) 34416; (41656) 34715.

E-mail заказчика: kanc@solov.ru

1.3 Основания для проведения работ

Основание для проведения работ обусловлено заявкой на проведения анализа защищенности информации на предприятии и разработки рекомендаций по ее улучшению, а также составление документации по обеспечению ИБ.

1.4 Плановые сроки начала и окончания работы

Срок начала работ: 06 февраля 2016 года.

Срок окончания работ: июнь 2017 года.

В процессе разработки сроки могут быть уточнены.

1.5 Источники и порядок финансирования

1.6 Порядок оформления и предъявления заказчику результатов работ

Работы по анализу и разработке рекомендаций, а также составленная документация сдаются после окончания процесса разработки. Заказчику предоставляется итоговый документ, а именно политика безопасности предприятия.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Назначение системы

Политика безопасности предприятия предназначена для регулирования управления, защиты и распределение ценной информации.

2.2 Цели создания системы

Целью создания политики безопасности является: обеспечить управление и поддержку в области информационной безопасности, защиту информации предприятия и обеспечение эффективной работы всего информационно-вычислительного комплекса.

Продолжение ПРИЛОЖЕНИЯ Г

3 ХАРАКТЕРИСТИКА ОБЪЕКТОВ АВТОМАТИЗАЦИИ

3.1 Краткие сведения об объекте автоматизации

Объектом автоматизации является само предприятие, а именно, его обособленное подразделение и вся информация, функционирующая на нем.

3.2 Сведения об условиях эксплуатации и о характеристике окружающей среды

Политика информационной безопасности является документом в системе управления информационной безопасностью (СУИБ) предприятия, выступающий в качестве одного из ключевых механизмов безопасности.

Политика безопасности должна быть внедрена на предприятии. С требованиями и правилами этих документов должен быть ознакомлен каждый сотрудник. За их невыполнение предусматривается ответственность, прописанная в политике безопасности.

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1 Требования к системе в целом

4.1.1 Требования к структуре и функционированию системы

Согласно отечественному стандарту ГОСТ Р ИСО/МЭК 17799-2005, политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к управлению информационной безопасностью. В соответствии с указанным стандартом, необходимо, чтобы политика информационной безопасности предприятия как минимум включала:

– определение информационной безопасности, её общих целей и сферы действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

– изложение целей и принципов информационной безопасности, сформулированных руководством;

– краткое изложение наиболее существенных для организации политик безопасности, принципов, правил и требований, например, таких как:

– соответствие законодательным требованиям и договорным обязательствам;

– предотвращение появления и обнаружение вирусов и другого вредоносного программного обеспечения;

– управление непрерывностью бизнеса;

– ответственность за нарушения политики безопасности;

– определение общих и конкретных обязанностей сотрудников в рамках управления информационной безопасностью, включая информирование об инцидентах нарушения информационной безопасности;

– ссылки на документы, дополняющие политику информационной безопасности, например, более детальные политики и процедуры для конкретных информационных систем, а также правила безопасности, которым должны следовать пользователи.

Для того чтобы политика информационной безопасности не оставалась только «на бумаге» необходимо, чтобы она была:

– непротиворечивой – разные документы не должны по-разному описывать подходы к одному и тому же процессу обработки информации;

– не запрещала необходимые действия – в таком случае неизбежные массовые нарушения приведут к дискредитации политики информационной безопасности среди пользователей;

– не налагала невыполнимых обязанностей и требований.

4.1.2 Требования к численности и квалификации персонала системы Политика информационной безопасности компании должна быть утверждена руководством, издана и доведена до сведения всех сотрудников в доступной и понятной форме.

Следовательно, политика безопасности регулирует деятельность всего обособленного подразделения, т.е. всех работников.

В организации должно быть назначено лицо, ответственное за политику безопасности, отвечающее за её эффективную реализацию и регулярный пересмотр.

4.1.3 Требования к патентной чистоте

Требования к патентной чистоте определяются на основе статей части 4 Гражданского кодекса Российской Федерации, раздел VII «Права на результаты интеллектуальной деятельности и средства индивидуализации».

Политика безопасности создается конкретно для данного обособленного подразделения впервые.

4.1.4 Требования к стандартизации и унификации

При создании политики безопасности должны быть учтены следующие стандарты:

ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ГОСТ 15408-02 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

ГОСТ Р ИСО/МЭК 27001. «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования»

ГОСТ Р ИСО/МЭК 27002 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»

ГОСТ Р ИСО/МЭК 27003 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности»

ГОСТ Р ИСО/МЭК 27003-2012. Приложение D. Структура политики

4.2 Требования к функциям, выполняемым системой

4.2.1 Перечень функций

Политика безопасности предприятия должна описывать:

– назначение политики информационной безопасности;

– основные принципы обеспечения ИБ;

– соответствие ПБ действующему законодательству;

– порядок подготовки персонала по вопросам информационной безопасности и допуска его к работе;

– защищаемые информационные ресурсы предприятия;

– политика использования паролей;

– политика реализации антивирусной защиты;

– ответственность нарушителей ПБ;

– роли и обязанности должностных лиц, отвечающих за ИБ предприятия

– политика обращения с информацией, составляющей коммерческую тайну или являющейся персональными данными;

– требования к помещениям, в которых проводятся совещания по секретной тематике и обрабатывается соответствующая информация;

– политика использования сети Интернет;

– политика приобретения, установки, модификации и обновления программного обеспечения;

– политика использования электронно-цифровой подписи и инфраструктуры публичных ключей;

– требования к подсистемам идентификации, аутентификации.

4.2.2 Сферы ответственности

Группа руководителей высшего эвена отвечает за обеспечение соответствующей проработки информации во всей организации.

Каждый руководитель высшего звена отвечает за то, чтобы сотрудники, работающие под его руководством, осуществляли защиту информации в соответствии со стандартами организации.

Начальник отела безопасности консультирует группу руководителей высшего звена, оказывает экспертную помощь сотрудникам организации и обеспечивает доступность отчетов о состоянии информационной безопасности.

Каждый сотрудник организации отвечает за информационную безопасность как часть выполнения своих должностных обязанностей.

Инциденты информационной безопасности не должны приводить к серьезным непредвиденным затратам или серьезным срывам работы служб и деятельности предприятия.

Потери из-за мошенничества должны быть известны и находиться в рамках приемлемых ограничений.

Вопросы информационной безопасности не должны оказывать неблагоприятного влияния на прием заказчиками продукции и услуг.

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

5.1 Перечень стадий и этапов работ по созданию системы

Политика – это общие намерения и указания, официально выраженные руководством. Содержание политики управляет действиями и решениями, касающимися предмета политики. Политика безопасности должна быть иерархически организована. Политика безопасности организации является политикой высшего уровня. Она подкрепляется более конкретными политиками, включая политику информационной безопасности и политику системы менеджмента информационной безопасности. В свою очередь, политика информационной безопасности может подкрепляться более детальными политиками по конкретным предметам, относящимся к аспектам информационной безопасности.

Содержание политики основано на контексте, в котором работает организация. В частности, при разработке любой политики в рамках основ политики нужно учитывать следующее:

– цели и задачи организации;

– стратегии, адаптированные для достижения этих целей;

– структуру и процессы, адаптированные организацией;

– цели и задачи, связанные с предметом политики;

– требования связанных политик более высокого уровня.

Политики могут иметь следующую структуру:

Краткое изложение политики – общее описание из одного-двух предложений.

Введение – краткое объяснение предмета политики.

Область действия –описывает части или действия организации, находящиеся под влиянием политики. При необходимости в пункте «Область действия» перечисляются другие политики, подкрепляемые данной политикой.

Цели – описание назначения политики.

Принципы – описание правил, касающихся действий и решений для достижения целей. В некоторых случаях может быть полезным определить ключевые процессы, связанные с предметом политики, и затем – правила выполнения процессов.

Сферы ответственности – кто отвечает за действия по выполнению требований политики. В некоторых случаях этот пункт может содержать описание организационных соглашений, а также сферы ответственности лиц с определенными ролями.

Ключевые результаты – описание результатов, получаемых предприятием, если цели достигнуты. Связанные политики – описание других политик, относящихся к достижению целей, обычно с представлением дополнительных подробностей, касающихся отдельных предметов.

5.2 Сроки выполнения

Разработка информационной системы определяется периодом с сентября 2016 по июнь 2017.

5.3 Состав организации исполнителя работ

Исполнителем всех вышеперечисленных работ является студент ФГБОУ ВО Амурский Государственный Университет Нечипоренко Анна Сергеевна.

5.4 Вид и порядок экспертизы технической документации

Вид и порядок экспертизы технической документации определяет Заказчик в одностороннем порядке.

Будет осуществлена проверка всей документации на плагиат.

6 ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ

Приемка и контроль подученной в ходе разработки системы будет осуществляться по следующим пунктам:

– анализ готовой системы;

– сравнение разработанной системы с техническим заданием на ее разработку, с целью определения выполнения всех предъявленных в нем требований;

– выполнение доработки и изменений системы при необходимости;

– опытная эксплуатация системы в режиме бета-тестирования;

– доработка системы и исправление ошибок;

Приемка работ осуществляется государственной аттестационной комиссией ФГБОУ ВО «АмГУ», в соответствие с календарным планом и учебной программной.

7 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ

На этапе внедрения необходимо не просто довести содержание ПБ до сведения всех сотрудников организации, но также провести.

Чтобы внедрение завершилось успешно, должна быть создана проектная группа по внедрению ПБ, действующая по согласованному плану в соответствии с установленными сроками выполнения работ.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

8.1 Перечень подлежащих обработке документов

В конечном итоге заказчик получает:

– техническое задание;

– разработанную политику безопасности;

– итог анализа угроз и уязвимостей;

– рекомендации по повышению уровня защищенности ИБ.

8.2. Перечень документов на машинных носителях

Документация из пункта 8.1 должна быть представлена на машинных носителях.

9 ИСТОЧНИКИ РАЗРАБОТКИ

Источниками разработки автоматизированной системы являются:

1 Галатенко В. А. Основы информационной безопасности: Курс лекций. — М.: ИНТУИТ.ру, 2003.- 280 с.

2 Законодательно-правовое и организационно-техническое обеспечение информационной безопасности АС и ИВС / Котенко И. В., Котухов М. М., Марков А. С. и др. Под ред. И. В. Котенко. - СПб: ВУС, 2000. - 190 с.

3 Комментарии к Российскому стандарту ГОСТ Р ИСО/МЭК 15408-2002 «Критерии оценки безопасности информационных технологий» / Долинин М. Ю., Кобзарь М. Т., Лыков В. А. и др. - М.: ФГУП «ЦНИИАТОМИН-ФОРМ», 2003. - 38 с.

4 Медведовский И. Д. Программные средства проверки и создания политики безопасности. — SecurityLab, 2004. — http:/ /www.security-hb.ru/42546.html

5 Политика безопасности при работе в Интернет: Техническое руководство / Б. Гутман, Р. Бэгвилл; Пер. с англ. Казенова В. Н. — NIST Special Publication 800-12 - 42 с.