Министерство образования и науки Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Южно-Уральский государственный университет
(национальный исследовательский университет)»

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2017 г.

Организация защиты информационной системы обработки персональных данных "Сотрудники и резиденты" в государственном бюджетном учреждении "Инновационный бизнес-инкубатор"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 501
_____ Каретников, И. А.
_____ 2017 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2017 г.

Челябинск 2017

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АРМ – автоматизированное рабочие место;
АС – автоматизированная система;
ВТСС – вспомогательные технические средства и системы;
ГБУ – государственное бюджетное учреждение;
ЗИ – защита информации;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
ИТ – информационные технологии;
МСЭ – межсетевой экран;
НСД – несанкционированный доступ;
ОТСС – основные технические средства и системы;
ПДн – персональные данные;
ПО – программное обеспечение;
РД – руководящие документы;
РФ – Российская Федерация;
СВТ – средства вычислительной техники;
ФЗ – Федеральный закон;
ФСБ – Федеральная служба безопасности;
ФСТЭК – Федеральная служба по техническому и экспортному контролю;

Базовые угрозы информационной безопасности – нарушение конфиденциальности, нарушение целостности и отказ в обслуживании;

Угроза – действие, которое потенциально может привести к нарушению безопасности. Свойством угрозы является перечень уязвимостей, при помощи которых может быть реализована угроза;

Уязвимость – это слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы. Свойствами уязвимости являются: вероятность (простота) реализации угрозы через данную уязвимость и критичность реализации угрозы через данную уязвимость;

Критичность ресурса – степень значимости ресурса для информационной системы, т.е. как сильно реализация угроз информационной безопасности на ресурс повлияет на работу информационной системы. Задается в деньгах;

Критичность реализации угрозы – степень влияния реализации угрозы на ресурс, т.е. как сильно реализация угрозы повлияет на работу ресурса. Задается в процентах;

Вероятность реализации угрозы через данную уязвимость в течение года – степень возможности реализации угрозы через данную уязвимость в тех или иных условиях. Указывается в процентах.

ВВЕДЕНИЕ

В век информационных технологий особую важность приобретает информация. Именно обработка информации, на сегодняшний день является одним из наиболее трудоемких процессов, особенно если нужно обрабатывать персональные данные.

Работа предприятия не возможна без обработки данных о сотрудниках, контрагентах, клиентах и т.д. Эта информация является персональными данными, которые в соответствии с Федеральным законом №152 "О персональных данных" от 27.07.2006 [1] необходимо защищать.

Таким образом, актуальность моей работы обусловлена необходимостью организации системы защиты информационной системы обработки персональных данных в ГБУ «Инновационный бизнес-инкубатор»

Объектом выпускной квалификационной работы является ГБУ «Инновационный бизнес-инкубатор».

Предметом выпускной квалификационной работы является информационная система обработки персональных данных в данной организации.

Целью дипломной работы является выбор и обоснование ряда мер по защите информационной системы обработки персональных данных.

В соответствии с поставленной целью необходимо решить следующие задачи:

- проанализировать информационную систему ГБУ «Инновационный бизнес-инкубатор», с целью обоснования создания системы защиты информационной системы обработки персональных данных;
- рассмотреть теоретические аспекты СЗИ;
- разработать проект по созданию системы защиты информационной системы обработки персональных данных в ГБУ «Инновационный бизнес-инкубатор».

1 АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ГБУ «ИННОВАЦИОННЫЙ БИЗНЕС-ИНКУБАТОР»

1.1 Разработка технического паспорта

Для создания системы защиты информации в начале необходимо сформировать общее представление об объекте защиты. Для этого было проведено предпроектное обследование, в результате которого был составлен технический паспорт предприятия (Приложение А).

В техническом паспорте приведены составы ОТСС, ВТСС, схемы их размещения, перечень установленных средств защиты информации, программного обеспечения, расположение линий передач.

В качестве объекта защиты была выбрана информационная система персональных данных «Сотрудники и резиденты» ГБУ «Инновационный бизнес-инкубатор»

1.2 Разработка модели деятельности

В ходе анализа работы ИСПДн «Сотрудники и резиденты» была построена модель деятельности организации (Приложение Е). В этой модели отображаются основные этапы технологического процесса обработки защищаемой информации от подготовки к обработке информации ограниченного доступа до сохранения результатов этой обработки.

Данная модель необходима для выявления потоков информации ограниченного доступа и построения эффективной защиты ИСПДн «Сотрудники и резиденты».

1.3 Выявление защищаемой информации

В ходе проведенного предпроектного обследования, ознакомления с информацией ограниченного доступа и организационно-распорядительной документацией был и в рамках выпускной квалификационной работы был разработан перечень персональных данных, подлежащих защите в информационной системе обработки персональных данных «Сотрудники и резиденты» №58 от 28.01.2017 г. (Приложение Б);

В целях исполнения требований Федерального закона от 27.07.2006г. №152-ФЗ «О персональных данных» [1], руководствуясь постановлением правительства Российской Федерации от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [2] для ИСПДн «Сотрудники и резиденты» был определён 4 уровень защищенности, в соответствии с актом №.87 от 02.02.2017 (Приложение Ж).

1.4 Описание информационной системы

В информационной системе ГБУ «Инновационный бизнес-инкубатор» можно выделить организационные, правовые и программно-аппаратные меры.

Организационные меры включает в себя такие документы как должностные инструкции персонала, отделов, по эксплуатации программного обеспечения и технических средств, инструкции по проведение контрольных или внештатных мероприятий, положения об отделах, системах взаимодействия с персоналом.

Правовые меры включают в себя свод определенных нормативно правовых документов, регулирующих как деятельность организации, так и информационных процессов, протекающих в ней относительно обеспечения защиты информации. Включающие в себя:

- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [3];
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [4];
- Федеральный закон «О персональных данных» [1];
- Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [2];

Программно-аппаратные меры, это комплекс программно-аппаратных средств, обеспечивающих работу и защиту информационной системы. Для описания информационной системы была проведена её инвентаризация, результаты которой представлены в таблицах 1.1 и 1.2.

Таблица 1.1 - Аппаратное обеспечение

Наименование устройства	Фирма/производитель, модель	Заводской/ инвентаризационный номер
ОТСС		
Системный блок	Zalman Z3	ZZ14221096153
НЖМД	Seagate ST2000VM003	ST-0F54H274112
Монитор	Acer G236HLBbid	G21986lA1819289
Клавиатура	Logitech Keyboard K120	LK21KS5214AH
Мышь	Oklick 205M	OM93751621A5
Принтер	Xerox Phaser 3260DNI	XP21864041FD
ИБП	APC by Schneider Electric Back-UPS 500	AS261BU43CK
ВТСС		
Системный блок	Zalman Z3	ZZ53F101A9
Монитор	Acer G236HLBbid	AG185201GJ
Клавиатура	Logitech Keyboard K120	LK391B84
Мышь	Oklick 205M	OK21K2912K

Продолжение таблицы 1.1.

Наименование устройства	Фирма/производитель, модель	Заводской/ инвентаризационный номер
ВТСС		
Системный блок	Zalman Z3	ZZ53B261C6
Монитор	Acer G236HLBbid	BEJE2241SX
Клавиатура	Logitech Keyboard K120	LK14A64K
Мышь	Oklick 205M	OK21K6932A
МФУ	Xerox Phaser 3260DNI	XP306125D
Телефонный аппарат	Panasonic KX-TS2365RU	PKT216S4B
Телефонный аппарат	Panasonic KX-TS2365RU	PKV366S7B
Датчик пожарной сигнализации	б/н	
Датчик пожарной сигнализации	б/н	
Коммутатор	D-link DES-1008D/K3	DL125OF2157
Роутер	TP-LINK TL-WR841N	TP30519

Далее в таблице 1.2 указано установленное программное обеспечение

Таблица – 1.2. Программное обеспечение

Наименование	Версия
Microsoft Windows 7 Professional SP1	6.1.7601.22616
Microsoft Office 2016	2016
Kaspersky Endpoint Security 10 для Windows	10.2.5.3201
КриптоПро CSP	3.6.1
Secret Net 7	7
TrustAccess	1.3

1.5. Выявление объектов защиты

В результате анализа технологического процесса обработки информации, а так же на основе перечня защищаемой информации были выделены объекты защиты и составлен следующий их перечень:

- автоматизированное рабочее место, где обрабатывается защищаемая информация;

- средства отображения информации;
- средства ввода-вывода информации;
- система бесперебойного питания АРМ;
- носители информации;
- линии и средства связи, системы обеспечения функционирования средств вычислительной техники и деятельности организации;
- персонал.

Более подробно перечень объектов защиты представлен в техническом паспорте (Приложении А).

1.6. Перечень мер защиты информации для системы защиты ИСПД

В соответствии с постановлением правительства Российской Федерации №1119 от 01.11.12 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:

- организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;
- обеспечение сохранности носителей персональных данных;
- утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;
- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Для обеспечения данных требований в рамках ВКР был создан приказ «Об организации работ по обеспечению безопасности персональных данных в ГБУ «Инновационный бизнес-инкубатор» (Приложение И).

1.7. Разработка частной модели угроз и уязвимостей для важных объектов защиты

Модель угроз информационной безопасности содержит систематизированный перечень угроз безопасности персональных данных при их обработке в информационных системах персональных данных.

Для того, чтобы выявить наиболее важные угрозы информационной безопасности организации, из большого количества возможных угроз сначала выделим важные объекты защиты информации, угроз безопасности персональных данных при их обработке в ИСПДн относительно защиты персональных данных:

- персонал;
- автоматизированные рабочие места сотрудников на которых обрабатывается защищаемая информация.

Далее для выбранных объектов защиты информации выделим наиболее существенные угрозы информационной безопасности, для этого воспользуемся базовой моделью угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанной ФСТЭК России [3]. И составим частную модель угроз информационной системы персональных данных «Сотрудники и резиденты»

1.7.1. Вероятность реализации угроз безопасности персональных данных

Для определения актуальных угроз воспользуемся методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанной ФСТЭК России [4].

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

Для определения актуальных угроз безопасности обработке в ИСПДн:
- определяется уровень исходной защищенности ИСПДн;
- определяется вероятность реализации рассматриваемых угроз;
- определяется возможность реализации угрлозы;
- оценивается опасность угроз в ИСПДн;
- составляется перечень актуальных угроз для данной ИСПДн;

1.7.2. Определение уровня исходной защищенности ИСПДн

Проведем оценку уровня защищенности на оценке исходных технических и эксплуатационных характеристик ИСПДн, представленных в таблице 1.3.

Таблица 1.3 – Исходный уровень защищенности

Технические и эксплуатационные характеристики	Уровень защищенности
По территориальному размещению	Высокий
По наличию соединения с сетями общего пользования	Средний
По встроенным (легальным) операциям с записями баз персональных данных	Низкий
По разграничению доступа к персональным данным	Средний
По наличию соединений с другими базами ПДн иных ИСПДн	Средний
По уровню (обезличивания) ПДн	Низкий

Продолжение таблицы 1.3

Технические и эксплуатационные характеристики	Уровень защищенности
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Высокая
По наличию соединений с другими базами ПДн иных ИСПДн	Средний
По уровню (обезличивания) ПДн	Низкий
По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки	Высокая

Данная ИСПДн имеет средний уровень исходной защищенности, так как не менее 70% характеристик соответствуют уровню не ниже «Средний», следовательно, показатель исходной защищенности Y1 = 5.

1.7.3. Определение вероятность реализации угроз в ИСПДн

Для определения актуальных угроз воспользуемся методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, разработанной ФСТЭК России [4].

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

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

Вводятся четыре вербальных градации этого показателя:

- маловероятно – отсутствуют объективные предпосылки для осуществления угрозы.
- низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию.
- средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;
- высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент Y2 , а именно: 0 – для маловероятной угрозы; 2 – для низкой вероятности угрозы; 5 – для средней вероятности угрозы; 10 – для высокой вероятности угрозы. Перечень актуальных угроз представлен в Приложении Ж.

1.7.4. Возможность реализации угроз

Для определения возможности реализации угрозы необходимо рассчитать коэффициент реализуемости угрозы (Y), который рассчитывается из оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2) и он будет определяться следующим соотношением Y = (Y1 + Y2) / 20

Определение возможности реализации угроз и оценка опасности угроз реализована в Приложении Ж.

Из полученной частной модели угроз были выделены следующие актуальные угрозы:

- угрозы несанкционированного доступа к информации: действия вредоносных программ; непреднамеренная модификация или уничтожение информации сотрудникам; установка ПО не связанного с исполнением служебных обязанностей;
- угрозы преднамеренных действий внутренних нарушителей: разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке;
- угрозы несанкционированного доступа по каналам связи: угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.; угрозы типа «Отказ в обслуживании».

1.8. Разработка технического задания на создание системы защиты ИСПДн «Сотрудники и резиденты»

В ходе проведенного предпроектного обследования и на основе полученной информации было разработано техническое задание на организацию системы защиты ИСПДн «Сотрудники и резиденты» (приложение Б).

Техническое задание разрабатывалось на основании ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» [5] и содержит следующие разделы:

- общие сведения;
- назначение и цели совершенствования системы;
- характеристика объектов защиты;
- требования к ИСПДн;
- состав и содержание работ по совершенствованию системы;
- порядок контроля и приемки системы;
- требования к составу и содержанию работ по подготовке объекта защиты – к вводу ИСПДн в действие;
- требования к документированию;
- источники разработки.

1.9. Безопасность жизнедеятельности

В связи с тем, что сотрудником необходимо работать в офисе за персональным компьютером, для них необходимо обеспечить безопасность их жизнедеятельности в организации.

Условия труда пользователя, работающего с персональным компьютером, определяются:

- особенностями организации рабочего места;
- условиями производственной среды;
- характеристиками информационного взаимодействия человека и персональных электронно-вычислительных машин.

1.9.1. Рекомендации по организации рабочего места пользователя

Рассмотрим основные нормативные документы и приведем некоторые рекомендации по организации рабочего места пользователя.

1.9.1.1. Рекомендации по выбору помещения для размещения рабочего места

Во время работы с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является верно спроектированное помещение, в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03 [6] помещения для эксплуатации ПЭВМ должны отвечать следующим требованиям:

- помещения должны иметь естественное и искусственное освещение;
- естественное и искусственное освещение должно соответствовать требованиям действующей нормативной документации;
- площадь на одно рабочее место пользователей ПЭВМ с ВДТ на базе плоских дискретных экранов (жидкокристаллические, плазменные), по СанПиН 2.2.2/2.4.1340-03, должно быть – 4,5 $м^2$ и 6 $м^2$ для ВДТ на базе ЭЛТ;
- для внутренней отделки интерьера помещений, где расположены ПЭВМ, должны использоваться диффузно-отражающие материалы с коэффициентом отражения для потолка – 0,7−0,8; для стен – 0,5−0,6; для пола – 0,3−0,5;
- помещения, где размещаются рабочие места с ПЭВМ, должны быть оборудованы защитным занулением или заземлением в соответствии с техническими требованиями по эксплуатации;
- не допускается расположение рабочих кабинетов, оборудованных ПЭВМ, в полуподвальных и подвальных помещениях.

Не следует размещать рабочие места с ПЭВМ вблизи силовых кабелей и вводов, высоковольтных трансформаторов, технологического оборудования, чтобы избежать появления помех, нарушающих функционирование ПЭВМ.

1.9.1.2. Требования к микроклимату

Для рабочих мест, на которых работа с ПЭВМ является основным видом выполняемых работ и связана с непрерывным эмоциональным напряжением, согласно СанПиН 2.2.2/2.4.1340-03 должны быть обеспечены оптимальные параметры микроклимата для работ категории Iа (Таблица 1.4). Параметры требований к микроклимату для работ различных категорий приведены в СанПиН 2.2.4.3359-16 [7].

Таблица 1.4 – Гигиенические требования к микроклимату производственных помещений (СанПиН 2.2.4.3359-16).

Период года	Категория работ по уровням энергозатрат, Вт	Температура воздуха, °С	Температура поверхностей, °С	Относительная влажность воздуха, %	Скорость движения воздуха, м/с
Холодный	Iа (до 139)	22 – 24	21 – 25	60 – 40	0,1
Теплый	Iа (до 139)	23 – 25	22 – 26	60 – 40	0,1

В соответствии с СанПиН 2.2.4.3359-16, в помещениях, оборудованных ПЭВМ, должна проводиться ежедневная влажная уборка, а также проветривание после каждого часа работы на ПЭВМ.

1.9.1.3. Требования к уровням шума

При работе на ПЭВМ источниками шума являются:
- источник бесперебойного питания;
- системный блок ПЭВМ;
- работающие принтеры и многофункциональные устройства.

Уровень шума на рабочих местах, при выполнении основных и вспомогательных производственных работ с использованием ПЭВМ не должен превышать показателей, устанавливаемых нормами СанПиН 2.2.2/2.4.1340-03 предельно допустимых значений для данных видов работ в соответствии с действующими санитарно-эпидемиологическими нормативами.

В соответствии с нормами, которые ограничивают предельно допустимое звуковое давление для рабочих мест, оснащённых ПЭВМ: шумящее оборудование, уровни шума которого превышают нормативные, должно размещаться вне помещений с ПЭВМ.

В соответствии с СанПин 2.2.4.3359-16 уровни шума на рабочих местах не должны превышать 80дБА.

1.9.1.4. Требования к освещению

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное освещение, не вызывающее раннего переутомления. Работа программиста требует

большой зрительной нагрузки, поэтому необходимо применять естественное освещение совместно с искусственным.

Согласно СанПиН 2.2.2/2.4.1340-03 рабочие столы следует размещать таким образом, чтобы ВДТ были ориентированы боковой стороной к световым проемам, чтобы естественный свет падал преимущественно слева. Искусственное освещение в помещениях для эксплуатации ПЭВМ должно осуществляться системой общего равномерного освещения. В производственных и административно-общественных помещениях, в случаях преимущественной работы с документами и бумагами, следует применять системы комбинированного освещения.

Освещенность на поверхности рабочего стола должна быть 300−500 лк. Освещенность поверхности экрана не должна быть более 300 лк., освещение не должно создавать бликов на поверхности экрана.

Для освещения помещений с ПЭВМ рекомендуется применять светильники с зеркальными параболическими решетками, укомплектованными электронными пускорегулирующими аппаратами (ЭПРА). Общее освещение при использовании люминесцентных светильников следует выполнять в виде сплошных или прерывистых линий светильников, расположенных сбоку от рабочих мест, параллельно линии зрения пользователя и линии оконных проёмов при рядном расположении рабочих мест, оснащённых ПЭВМ с ВДТ. При периметральном расположении компьютеров линии светильников должны располагаться локализовано над рабочим столом ближе к его переднему краю, обращенному к оператору. Коэффициент пульсации не должен превышать 5%.

Для обеспечения нормируемых значений освещенности в помещениях для использования ПЭВМ следует проводить чистку стекол оконных рам и светильников не реже двух раз в год и проводить своевременную замену перегоревших ламп.

1.9.1.5. Общие требования к организации рабочих мест

Рабочее место оператора ЭВМ проектируется согласно СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы».

При размещении рабочих мест с ПЭВМ расстояние между рабочими столами с видеомониторами (в направлении тыла поверхности одного экрана и экрана другого монитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями экранов – не менее 1,2 м.

Рабочие места с ПЭВМ в помещениях с источниками вредных производственных факторов должны размещаться в изолированных кабинах с организованным воздухообменом.

Рабочие места с ПЭВМ при выполнении работы, требующей значительного умственного напряжения или высокой концентрации внимания, рекомендуется изолировать друг от друга перегородками высотой 1,5−2,0 м.

Экран монитора должен находиться от глаз пользователя на расстоянии 600−700 мм, но не ближе 500 мм с учетом размеров алфавитно-цифровых знаков и символов.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей, характера выполняемой работы.

При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики. Поверхность рабочего стола должна иметь коэффициент отражения 0,5−0,7.

При организации рабочих мест необходимо использовать рабочий стул (кресло) обеспечивающий поддержание рациональной рабочей позы при работе на ПЭВМ, позволяющий изменять позу с целью снижения статического напряжения мышц шейно-плечевой области и спины для предупреждения развития утомления. Тип рабочего стула (кресла) следует выбирать с учетом роста пользователя, характера и продолжительности работы с ПЭВМ.

Рабочий стул (кресло) должно быть обеспеченно подъемно-поворотным механизмом, также оно должно быть регулируемым по высоте и углам наклона сиденья и спинки, а также расстояния спинки от переднего края сиденья, при этом регулировка каждого параметра должна быть независимой, легко осуществляемой и иметь надежную фиксацию.

Поверхность сиденья, спинки и других элементов стула (кресла) должна быть полумягкой, с нескользящим, слабо электризующимся и воздухопроницаемым покрытием, обеспечивающим легкую очистку от загрязнений.

Высота рабочей поверхности стола должна регулироваться в пределах 680−800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.

Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, высота должна быть равной 725 мм.

Рабочий стол должен иметь пространство для ног высотой не менее 600 мм, шириной – не менее 500 мм, глубиной на уровне колен – не менее 450 мм и на уровне вытянутых ног – не менее 650 мм.

Конструкция рабочего стола должна обеспечивать оптимальное размещение на рабочей поверхности используемого оборудования с учетом его количества и конструктивных особенностей (размер ВДТ и ПЭВМ, клавиатуры, и др.), характера выполняемой работы. При этом допускается использование рабочих столов различных конструкций, отвечающих современным требованиям эргономики.

Конструкция стула (кресла) должна обеспечивать:

- ширину и глубину поверхности сиденья не менее 400 мм;
- поверхность сиденья с закругленным передним краем;
- регулировку высоты поверхности сиденья в пределах 400−550 мм и углам наклона вперед до 15°, и назад до 5°;

- высоту опорной поверхности спинки 300±20 мм, ширину – не менее 380мм и радиус кривизны горизонтальной плоскости – 400 мм;

- угол наклона спинки в вертикальной плоскости в пределах ±30°;

- регулировку расстояния спинки от переднего края сиденья в пределах 260−400 мм;

- стационарные или съемные подлокотники длиной не менее 250 мм и шириной – 50−70 мм;

- регулировку подлокотников по высоте над сиденьем в пределах 230±30 мм и внутреннего расстояния между подлокотниками в пределах 350−500 мм.

Рабочее место пользователя ПЭВМ, согласно СанПиН 2.2.2.542-96 [8], следует оборудовать подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм, регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20°. Поверхность подставки должна быть рифленой и иметь по переднему краю бортик высотой 10 мм.

Клавиатуру следует располагать на поверхности стола на расстоянии 100−300 мм от края, обращенного к пользователю или на специальной, регулируемой по высоте рабочей поверхности, отделенной от основной столешницы.

1.9.2. Электробезопасность

По степени опасности поражения электрическим током согласно Правилам Устройства Электроустановок (ПУЭ) рабочее помещение относится к классу помещений с повышенной опасностью, так как имеется возможность одновременного прикосновения человека к имеющим соединения с землей металлоконструкциям здания с одной стороны и металлическим корпусам электрооборудования с другой.

Если физический доступ к токоведущим частям оборудования затруднен, то основной причиной возникновения данного опасного фактора может являться прикосновение к металлическим нетоковедущим частям (например, корпусу ПЭВМ), которые могут оказаться под напряжением в результате повреждения изоляции. В соответствии с правилами электробезопасности, должен осуществляться постоянный контроль состояния электропроводки, предохранительных щитов, шнуров, с помощью которых включаются в электросеть компьютеры, осветительные приборы, другие электроприборы.

Для защиты от случайного прикосновения к металлическим нетоковедущим частям оборудования, которые могут оказаться под напряжение применяют следующие меры:

- защитное заземление;
- зануление;
- изоляцию нетоковедущих частей;
- защитное экранирование.

Данные меры описаны в ГОСТ Р 12.1.019-2009 «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты» [9].

1.9.3. Пожарная безопасность

Горючие вещества и материалы, находящиеся в помещении: дерево (мебель), бумага (документы), ПЭВМ.

Возможными источниками зажигания могут быть тепловые проявления электрической энергии (короткое замыкание. высокие сопротивления, искровые разряды статического электричества и др.).

Источниками пожара может стать неисправность или нарушение правил эксплуатации электротехнического оборудования.

Для тушения возможного пожара помещение оборудовано одним ручным порошковым огнетушителем ОП-4.

В соответствии с Федеральным законом №123 «Технический регламент о требованиях пожарной безопасности» [10] были установлены следующие правила:

Организации, их должностные лица и граждане, нарушившие требования пожарной безопасности, несут ответственность в соответствии с законодательством Российской Федерации.

Наряду с настоящими Правилами, следует также руководствоваться иными нормативными документами по пожарной безопасности и нормативными документами, содержащими требования пожарной безопасности, утвержденными в установленном порядке.

Руководители организации и индивидуальные предприниматели на своих объектах должны иметь систему пожарной безопасности, направленную на предотвращение воздействия на людей опасных факторов пожара, в том числе их вторичных проявлений.

На каждом объекте должны быть разработаны инструкции о мерах пожарной безопасности для каждого взрывопожароопасного и пожароопасного участка (мастерской, цеха и т.п.) в соответствии с приложением данных правил.

Все работники организаций должны допускаться к работе только после прохождения противопожарного инструктажа, а при изменении специфики работы проходить дополнительное обучение по предупреждению и тушению возможных пожаров в порядке, установленном руководителем.

Руководители организаций или индивидуальные предприниматели имеют право назначать лиц, которые по занимаемой должности или по характеру выполняемых работ в силу действующих нормативных правовых актов и иных актов должны выполнять соответствующие правила пожарной безопасности либо обеспечивать их соблюдение на определенных участках работ.

Для привлечения работников предприятий к работе по предупреждению и борьбе с пожарами на объектах могут создаваться пожарно-технические комиссии и добровольные пожарные формирования.

Собственники имущества, лица, уполномоченные владеть, пользоваться или распоряжаться имуществом, в том числе руководители и должностные лица организаций, лица, в установленном порядке назначенные ответственными за обеспечение пожарной безопасности, должны:

- обеспечивать своевременное выполнение требований пожарной безопасности, предписаний, постановлений и иных законных требований государственных инспекторов по пожарному надзору;

- создавать и содержать на основании утвержденных в установленном порядке норм, перечней особо важных и режимных объектов и предприятий, на которых создается пожарная охрана, органы управления и подразделения пожарной охраны, а также обеспечивать в них непрерывное несение службы и использование личного состава и пожарной техники строго по назначению.

Во всех производственных, административных, складских и вспомогательных помещениях на видных местах должны быть вывешены таблички с указанием номера телефона вызова пожарной охраны.

Правила применения на территории организаций открытого огня, проезда транспорта, допустимость курения и проведения временных пожароопасных работ устанавливаются общеобъектовыми инструкциями о мерах пожарной безопасности.

В каждой организации распорядительным документом должен быть установлен соответствующий их пожарной опасности противопожарный режим, в том числе:

- определены и оборудованы места для курения;

- определены места и допустимое количество единовременно находящихся в помещениях сырья, полуфабрикатов и готовой продукции;

- установлен порядок уборки горючих отходов и пыли, хранения промасленной спецодежды;

- определен порядок обесточивания электрооборудования в случае пожара и по окончании рабочего дня;

- регламентированы:

- порядок проведения временных огневых и других пожароопасных работ;

- порядок осмотра и закрытия помещений после окончания работы;

- действия работников при обнаружении пожара;

- определен порядок и сроки прохождения противопожарного инструктажа и занятий по пожарно-техническому минимуму, а также назначены ответственные за их проведение.

В зданиях и сооружениях (кроме жилых домов) при единовременном нахождении на этаже более 10 человек должны быть разработаны и на видных местах вывешены планы (схемы) эвакуации людей в случае пожара, а также предусмотрена система (установка) оповещения людей о пожаре.

На объектах с массовым пребыванием людей (50 и более человек) в дополнение к схематическому плану эвакуации людей при пожаре должна быть разработана инструкция, определяющая действия персонала по обеспечению безопасной и быстрой эвакуации людей, по которой не реже одного раза в полугодие должны проводиться практические тренировки всех задействованных для эвакуации работников.

Световая, звуковая и визуальная информирующая сигнализация должна быть предусмотрена в помещениях, посещаемых данной категорией лиц, а также у ка-

ждого эвакуационного, аварийного выхода и на путях эвакуации. Световые сигналы в виде светящихся знаков должны включаться одновременно со звуковыми сигналами. Работники организаций, а также граждане должны:

- соблюдать на производстве и в быту требования пожарной безопасности, а также соблюдать и поддерживать противопожарный режим;
- выполнять меры предосторожности при пользовании газовыми приборами, предметами бытовой химии, проведении работ с легковоспламеняющимися (далее - ЛВЖ) и горючими (далее - ГЖ) жидкостями, другими опасными в пожарном отношении веществами, материалами и оборудованием;
- в случае обнаружения пожара сообщить о нем в подразделение пожарной охраны и принять возможные меры к спасению людей, имущества и ликвидации пожара.

Граждане предоставляют в порядке, установленном законодательством Российской Федерации, возможность государственным инспекторам по пожарному надзору проводить обследования и проверки принадлежащих им производственных, хозяйственных, жилых и иных помещений и строений в целях контроля за соблюдением требований пожарной безопасности.

Противопожарные системы и установки (противодымная защита, средства пожарной автоматики, системы противопожарного водоснабжения, противопожарные двери, клапаны, другие защитные устройства в противопожарных стенах и перекрытиях и т.п.) помещений, зданий и сооружений должны постоянно содержаться в исправном рабочем состоянии.

Устройства для самозакрывания дверей должны находиться в исправном состоянии. Не допускается устанавливать какие-либо приспособления, препятствующие нормальному закрыванию противопожарных или противодымных дверей (устройств).

1.9.4. Рекомендации по организации режима труда и отдыха пользователя

Режимы труда и отдыха при работе с ПЭВМ и ВДТ должны организовываться в зависимости от вида и категории трудовой деятельности согласно СанПиН 2.2.2/2.4.1340-03.

По виду трудовой деятельности работу оператора можно отнести к группе «А» – работа по считыванию информации с экрана ВДТ или ПЭВМ с предварительным запросом.

Для видов трудовой деятельности устанавливается три категории тяжести и напряженности работы с ВДТ и ПЭВМ.

Для группы А категории определяются по суммарному числу считываемых знаков за рабочую смену, но не более 60 000 знаков за смену:

- 1 категория – до 20 000 знаков;
- 2 категория – до 40 000 знаков;
- 3 категория – до 60 000 знаков.

Продолжительность обеденного перерыва определяется действующим законодательством о труде и правилами внутреннего распорядка предприятия.

Для обеспечения оптимальной работоспособности и сохранения здоровья профессиональных пользователей, на протяжении рабочей смены должны устанавливаться регламентированные перерывы. Время регламентированных перерывов в течении рабочей смены следует устанавливать в зависимости от ее продолжительности, вида и категории трудовой деятельности. Продолжительность непрерывной работы без регламентированного перерыва не должна превышать двух часов. При восьмичасовой рабочей смене и работе на ВДТ и ПЭВМ регламентированные перерывы следует устанавливать:

- для 1 категории работ через 2 ч. от начала рабочей смены и через 2 ч. после обеденного перерыва продолжительностью 15 мин. каждый;
- для 2 категории работ через 2 ч. от начала рабочей смены и через 1,5–2 ч. после обеденного перерыва продолжительностью 15 мин. каждый или продолжительностью 10 мин. через каждый час работы;
- для 3 категории работ через 2 ч. от начала рабочей смены и через 1,5−2,0 ч. после обеденного перерыва продолжительностью 20 мин. каждый или продолжительностью 15 мин. через каждый час работы.

Во время регламентированных перерывов с целью снижения нервно эмоционального напряжения, утомления зрительного анализатора, устранения влияния гиподинамии и гипокинезии, предотвращения развития познотонического утомления целесообразно выполнять комплексы упражнений для глаз, для улучшения мозгового кровообращения, для снятия утомления с плечевого пояса и рук, а также общего воздействия.

В случаях возникновения у пользователя зрительного дискомфорта и других неблагоприятных субъективных ощущений, несмотря на соблюдение санитарно-гигиенических, эргономических требований, режимов труда и отдыха следует применять индивидуальный подход в ограничении времени работ с ВДТ и ПЭВМ. Коррекцию длительности перерывов для отдыха или проводить смену деятельности на другую, не связанную с использованием ВДТ и ПЭВМ.

Организационные мероприятия, устраняющие причины возникновения пожаров: обучение рабочих и служащих противопожарным правилам, проведение лекций, инструкций и т.п. Технические мероприятия: соблюдение противопожарных правил и норм при устройстве оборудования отопления, вентиляции и т.д.

Мероприятия режимного характера: запрещение курения в не установленных местах, проведения сварочных работ в пожарных помещениях. Эксплуатационные мероприятия: правильная эксплуатация машин, транспорта, оборудования и правильное содержание зданий, территорий.

ВЫВОД ПО ПЕРВОЙ ГЛАВЕ

В ходе проведенного предпроектного обследования существующей системы защиты информации ГБУ «Инновационный бизнес-инкубатор», была проведена следующая работа:

- Составлен технический паспорт на обработку персональных данных;
- Разработана модель деятельности, отражающая процесс обработки информации ограниченного доступа;
- Разработан перечень персональных данных, подлежащих защите в информационной системе обработки персональных данных;
- Разработана модель угроз безопасности персональных данных и произведена оценка их актуальности;
- Разработано техническое задание на создание защиты информационной системы персональных данных в ГБУ «Инновационный бизнес-инкубатор»;
- Был проведен анализ мероприятий по безопасности жизнедеятельности на предприятии ГБУ «Инновационный бизнес-инкубатор»;

2. ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1. Обзор возможных методов устранения уязвимостей

Одним из важнейших этапов создания защиты информационной системы обработки персональных данных является определение методов и средств, которые необходимы для устранения выявленных угроз и уязвимостей, определенных в первой главе данной работы, и выбрать из них наиболее эффективные.

2.2. Угрозы несанкционированного доступа к информации

Следуя из ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» [11] несанкционированный доступ (НСД) к информации – деятельность, направленная на предотвращение получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Из результатов предпроектного обследования ясно, что в ГБУ «Инновационный бизнес-инкубатор» имеется высокая вероятность возникновения угроз связанных с НСД. Для защиты от данной угрозы необходимо использовать соответствующие программно-аппаратные средства защиты, которые позволят управлять доступом к автоматизированной системе, выполнять регистрацию и учет и обеспечивать целостность и неизменность программной среды.

Для того, чтобы выбрать необходимые программно-аппаратные средства проведем их сравнительный анализ. Сравнительный анализ программно-аппаратных СЗИ от НСД представлены в таблице 2.1.

Таблица 2.1. – Сравнение СЗИ от НСД

Критерии сравнения	Secret Net 7	Dallas Lock 8.0-K	Панцирь-К	СЗИ Аура 1.2.4.
Класс защищенности	По 3 классу защищенности	По 5 классу защищенности	По 5 классу защищенности	По 5 классу защищенности
Уровень контроля НДВ	По 2 уровню контроля	По 4 уровню контроля	По 4 уровню контроля	По 4 уровню контроля
Дополнительная аппаратная поддержка	есть	есть	есть	нет

Из выгодного соотношения цена/функциональность для минимизации угроз от НСД был выбран «Secret Net 7».

В качестве антивирусного ПО был выбран «Kaspersky Endpoint Security 10 для Windows», т.к в ГБУ «Инновационный бизнес-инкубатор» данное антивирусное ПО уже приобретено.

2.3. Угрозы несанкционированного доступа по каналам связи

Данная угроза заключается в передаче запросов сетевым узлам и анализе их ответов, в результате чего может быть получена топология сети, используемые порты, активные сетевые сервисы.

Из результатов предпроектного обследования стало ясно, что для ГБУ «Инновационный бизнес-инкубатор» актуальны угрозы сканирования направленные на выявления типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.

Для решения данной проблемы необходима установка межсетевого экрана. Межсетевой экран – это устройство обеспечения безопасности сети, которое осуществляет мониторинг входящего и исходящего сетевого трафика и на основании установленного набора правил безопасности принимает решения, пропустить или блокировать конкретный трафик. Проведем сравнительный анализ межсетевых экранов (Таблица 2.2).

Таблица 2.2 – сравнительный анализ межсетевых экранов

Характеристики	TrustAccess	Киберсейф: Межсетевой экран	VipNet Office Firewall
Класс МЭ	2	3	4
Наличие сертификата ФСТЭК	Да	Да	Да
Цена	От 4000 (1рабочее место)	От 15200 (25 рабочих мест)	От 15 700 (1 рабочее место)

По соотношению цена/функциональность и совместимости с СЗИ от НСД «Secret Net 7» для защиты выберем межсетевой экран «TrustAccess».

2.4. Угрозы преднамеренных действий внутренних нарушителей

Угрозы преднамеренных действий внутренних нарушителей являются наиболее распространенными и следовательно, наиболее важными с точки зрения защиты информации, так как именно сотрудники, допущенные к обработке информации ограниченного доступа являются нарушителями.

Для ГБУ «Инновационный бизнес-инкубатор» данный вид угроз актуален и рекомендуется выполнить следующие меры:

- Установить антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»;
- Установить СЗИ от НСД «Secret Net 7»»;
- Обеспечить резервное копирование информации, обрабатываемой на АРМ.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

Таким образом, в результате выявления уязвимостей на рассматриваемом объекте, приводящих к возможной реализации той или иной угрозы, были определены и рекомендованы следующие мероприятия, препятствующие возникновению неблагоприятных последствий от воздействия угроз.

Для решения угроз несанкционированного доступа к информации: установка антивирусного ПО «Kaspersky Endpoint Security 10 для Windows»; установка СЗИ от НСД «Secret Net 7»; обеспечение резервного копирование информации, обрабатываемой на АРМ.

Для решения угроз несанкционированного доступа по каналам связи необходимо установить межсетевой экран «TrustAccess».

Для решения угроз преднамеренных действий внутренних нарушителей необходимо: установка антивирусного ПО «Kaspersky Endpoint Security 10 для Windows»; установка СЗИ от НСД«Secret Net 7»; обеспечение резервного копирование информации, обрабатываемой на АРМ.

3. РАЗРАБОТКА ПРОЕКТА ОРГАНИЗАЦИИ ЗАЩИТЫ ИСПДН «СОТРУДНИКИ И РЕЗИДЕНТЫ» ГБУ «ИННОВАЦИОННЫЙ БИЗНЕС-ИНКУБАТОР»

3.1. Описание объекта

ГБУ «Инновационный бизнес-инкубатор» осуществляет реализацию областной целевой Программы развития малого и среднего бизнеса с целью содействия экономическому развитию региона. Из-за чего возникает необходимость обрабатывать и защищать персональные данные сотрудников и резидентов данной организации. В результате составлены следующие потоки защищаемой информации.

Таблица 3.1. – Потоки защищаемой информации

Входящая	Исходящая
1	2
Информация о клиентах	
Документооборот с другими отделами	

3.2. Резюме проекта

Проект разработан согласно утвержденному техническому заданию на создание системы защиты информационной системы персональных данных «Сотрудники и резиденты» ГБУ «Инновационный бизнес-инкубатор» (Приложение Б).

Для создания системы защиты необходимо разработать ряд организационных, инженерно-технических и программно-аппаратных мер. С помощью матрицы ответственности за каждым конкретным этапом работы зафиксированы ответственные лица.

Результатом проекта станет система защиты информационной системы персональных данных «Сотрудники и резиденты», соответствующая нормативно-правовым актам в области защиты персональных данных.

3.3. Цели и задачи проекта

Целями создания системы защиты информации ГБУ «Инновационный бизнес-инкубатор» являются:

- Предотвращение угроз, связанных с НСД;
- Предотвращение угроз несанкционированного доступа по каналам связи;
- Предотвращение угроз преднамеренных действий внутренних нарушителей;
- Осуществление защиты персональных данных в соответствии с нормативно-правовыми актами.

3.4. Объекты поставки проекта

3.4.1. Организационно-распорядительная документация

К существующим в организации организационно-распорядительным документам в области защиты информации в рамках ВКР было добавлено:

- Приказ «Об организации работ по обеспечению безопасности персональных данных в ГБУ «Инновационный бизнес-инкубатор» (Приложение И);
- Акт определения уровня защищенности ИСПДн «Сотрудники и резиденты» в ГБУ «Инновационный бизнес-инкубатор» (Приложение Ж);
- Модель угроз (Приложение З);
- Перечень персональных данных, подлежащих защите в информационной системе обработки персональных данных (Приложение В);
- Технический паспорт на разработку систему обработки персональных данных (Приложение А);
- Техническое задание на создание системы защиты персональных данных (Приложение Б);
- Модель деятельности (Приложение Е).

3.4.2. Программно-аппаратные и инженерно-технические меры

Для реализации проекта будут закуплены и установлены следующие программные средства:

- СЗИ от НСД «Secret Net 7»;
- Антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»;
- Межсетевой экран «TrustAccess»;

Так же были выполнены следующие инженерно-технические меры:

- Обеспечение резервного копирования информации, обрабатываемой на АРМ.

3.4.3. Обучение персонала

Для реализации проекта будет проведено обучение сотрудников работы с персональными данными, обучения основам работы с СЗИ от НСД и инструктаж по обеспечению информационной безопасности и антивирусной защите.

3.5. Риски проекта

Вероятность реализации угрозы через данную уязвимость в течение года: P(V), (%)

Критичность реализации угрозы через уязвимость: ER, (%)

Уровень угрозы Th (%), рассчитывается по формуле (1).

$$Th = \frac{ER \cdot P(V)}{10000} \quad (1)$$

Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh (%), рассчитывается по формуле (2):

$$CTh = 1 - \prod_{i=1}^{n}(1 - Th) \quad (2)$$

Далее в таблице 3.2 представлены риски реализации проекта.

Таблица 3.2 – риски реализации проекта

Риски / пути их реализации	Критичность ER	Вероятность P(V)	h	CTh
1. Риски изменений в стране, обществе				
1.1. Ухудшение политических и экономических характеристик и факторов:				0,647
– реформы в экономике и политике	10	5	0,005	
– изменение законодательства	30	20	0,06	
1.2. Изменение характеристик общества:				0,407
– здравоохранение и медицина, условия отдыха	25	5	0,012	
– возникновение негативного отношения сотрудников	80	50	0,4	
1.3. Влияние форс-мажорных обстоятельств:				
– стихийные бедствия и природные катаклизмы				
2. Риски окружения проекта в составе организации				
2.1. Изменение или недостаток бюджета проекта:				0,896
– задержки финансирования	90	50	0,45	
– отсутствие денежного резерва для реагирования на события рисков (в т.ч. для ликвидации отставания от графика)	90	90	0,81	
2.2. Недостаточная организованность работ				0,031
– срыв графиков работ, невыполнение сроков	10	10	0,01	
– нехватка рабочей силы	30	5	0,015	
– недооценка стоимости работ и использование финансов для других целей	30	2	0,006	
2.3. Риски персонала				0,035
– влияние личностных факторов (неумеренные амбиции участников проекта, переоценка собственных возможностей, преувеличение роли технологической стороны в ущерб менеджменту)	25	10	0,025	
– риск недоступности персонала, которому сложно подобрать замену (болезнь, увольнение и другие непредвиденные обстоятельства)	20	5	0,01	

Наиболее высокие риски проекта связаны с возможным изменением или недостатком бюджета.

3.6. Структура разбиения работ

Структура разбиения работ позволяет определить необходимы работы для реализации, установить структуру их выполнения и управления. Структура работ представлена на рисунке 3.1.

ИСПДн 1. Предпроектная стадия;

ИСПДн 1.1. Изучение существующих организационных мер обеспечения безопасности персональных данных;

ИСПДн 1.2. Разработка частной модели угроз;

ИСПДн 1.3. Категорирование и определение уровня защищенности ИСПДн;

ИСПДн 1.4. Анализ соответствия применяющихся мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных.

ИСПДн 2. Стадия проектирования;

ИСПДн 2.1. Разработка организационно-распорядительной документации;

ИСПДн 2.2. Приобретение СЗИ от НСД;

ИСПДн 2.3. Приобретение межсетевого экрана.

ИСПДн 3. Реализация;

ИСПДн 3.1. Установка и настройка СЗИ от НСД;

ИСПДн 3.2. Установка и настройка антивирусного ПО;

ИСПДн 3.3. Обучение пользователей;

ИСПДн 3.4. Контроль защищенности.

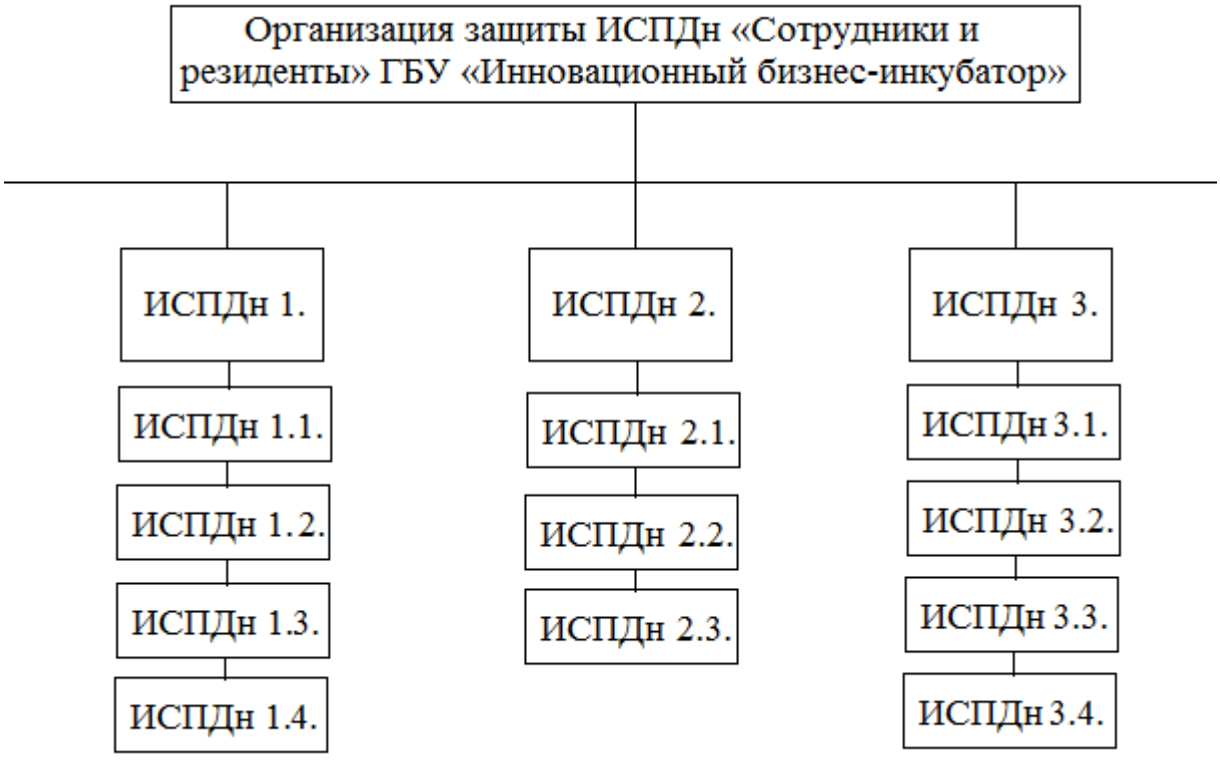


Рисунок 3.1 – Структура разбиения работ

3.7. Структурная схема организации проекта

Для совместной работы сотрудников, привлеченных к выполнению работ, была разработана структурная схема организации проекта (Рисунок 3.2).

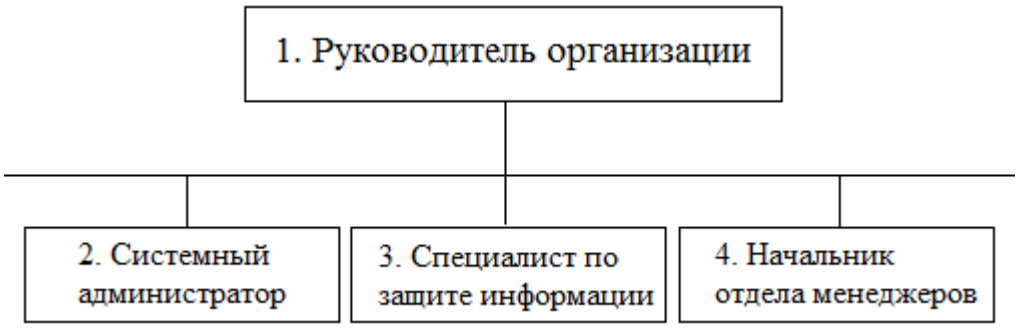


Рисунок 3.2 – Структурная схема организации проекта

3.8. Матрица ответственности

Для наглядности составим матрицу ответственности работ для исполнительней проекта (Таблица 3.3). Работа исполнителей делится на три группы: управление (У), исполнение (И), контроль (К).

Таблица 3.3 – Матрица ответственности

Исполнитель/Работа	1	2	3	4
ИСПДн 1.	К/У			
ИСПДн 1.1.	К		И	
ИСПДн 1.2.	К		И	
ИСПДн 1.3	К		И	
ИСПДн 1.4.	К		И	
ИСПДн 2.	К			
ИСПДн 2.1.	К		У/И	
ИСПДн 2.2.	К	И		
ИСПДн 2.3.	К	И		
ИСПДн 3.	К			
ИСПДн 3.1.	К			
ИСПДн 3.2.	К			
ИСПДн 3.3.	К			И
ИСПДн 3.4.	К			

3.9. Диаграмма Ганта и сетевой график

Диаграмма Ганта является одним из методов планирования проектов, иллюстрирует план и график работ. Для проекта усовершенствования СЗИ ГБУ «Инновационный бизнес-инкубатор» была построена диаграмма Ганта и представлена в Приложении Г.

На основании диаграммы Ганта видно, что на реализацию проекта понадобиться 43 дня.

Сетевой график – это динамическая модель проекта, отражающая последовательность и зависимость работ, необходимых для завершения проекта. Сетевой график для проекта организации защиты ИСПДн ГБУ «Инновационный бизнес-инкубатор» представлен в приложении Д.

3.10. Расчет бюджета проекта

В результате предпроектного обследования были выявлены уязвимости в системе, в связи с чем необходимо их устранить организовав систему защиты. Был проведен расчёт затрат на реализацию предложенных мер защиты. В таблице 3.4 представлена стоимость оборудования и программного обеспечения

Таблица 3.4 – Стоимость оборудования и программного обеспечения

Наименование	Количество	Цена за шт. (руб.)	Сумма (руб.)
СЗИ от НСД «Secret Net 7»	1	7 500	7 500
Межсетевой экран «TrustAccess»	1	4 500	4 500
		Итог	12 000

Стоимость реализации проекта приведена в таблице 3.5

Таблица 3.5. – Стоимость реализации проекта

Наименование	Стоимость (руб.)
Анализ существующей СЗИ	5 000
Разработка организационно-распорядительной документации	5 000
Установка и настройка СЗИ от НСД «Secret Net 7»	3 000
Установка и настройка антивирусного ПО «Kaspersky Endpoint Security 10 для Windows»	3 000
Итог	19 000

Затраты на реализацию проекта по организации системы защиты ИСПДн «Сотрудники и резиденты» в ГБУ «Инновационный бизнес-инкубатор» составили 31 000 рублей.

ВЫВОД ПО ТРЕТЕЙ ГЛАВЕ

По результатам выполненных работ разработан проект организации системы защиты ИСПДн «Сотрудники и резиденты» ГБУ “Инновационный бизнес-инкубатор”. Работы были разбиты в последовательности и иерархически структурированы. Каждой работе назначен ответственный за неё и/или исполнитель, структура разбиения работ наглядно представлена на сетевых графиках и диаграмме Ганта (Приложение Г). Осуществление работ по проекту завершается введением в эксплуатацию комплекса мер по обеспечению защиты персональных данных.

В результате расчета всех затрат на организацию защиты ИСПДн «Сотрудники и резиденты» ГБУ «Инновационный бизнес-инкубатор» необходимо 31 000 рублей, что позволит выполнить требования законодательства в области персональных данных, это значит, что проект по организации защиты ИСПДн ГБУ «Инновационный бизнес-инкубатор» целесообразен.

ЗАКЛЮЧЕНИЕ

В результате проведения выпускной квалификационной работы был проведен анализ состояния защиты информации на предприятии ГБУ «Инновационный бизнес-инкубатор». В ходе предпроектного обследования были выявлены уязвимости в существующей системе защиты информации и отсутствие части организационно-распорядительной документации в области защиты информации. В связи с чем были разработаны необходимые организационно-распорядительные документы и выбраны необходимые программно-аппаратные средства защиты информации.

Результатами выпускной квалификационной работы стали:

- Разработан технический паспорт на автоматизированную систему – был проведен осмотр помещений и технических средств, составлен их перечень и схемы расположения;
- Разработана модель деятельности предприятия – построены диаграммы, позволяющие выявить потоки защищаемой информации;
- Разработана модель угроз и уязвимостей для информационной системы персональных данных и рассчитаны риски на основе базовой модели угроз безопасности ФСТЭК и методики определения актуальных угроз ФСТЭК;
- Разработано техническое задание на организацию системы защиты ИСПДн в ГБУ«Инновационный бизнес-инкубатор» в соответствии с текущим законодательством в области обеспечения защиты персональных данных.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Федеральный закон «О персональных данных»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

2. Постановление правительства РФ «Об утверждении требований к за-щите персональных данных при их обработке в информационных системах персональных данных»: постановление правительства Российской Федерации от 01.11.2012 № 1119 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

3. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (выписка): утверждена заместителем директора ФСТЭК России 15.02.2008 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

4. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»: утверждена заместителем директора ФСТЭК России 14.02.2008 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.5

5. ГОСТ 34.602-1989. Техническое задание на создание автоматизированной системы. – М.: Изд-во стандартов, 1990. – 12 с.

6. СанПин 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислителным машинам и огранизации работы. – М.: Изд-во стандартов, 2003. – 36 с.

7. СанПин 2.2.4.3359-16. Санитарно-эпидемологические требования к физическим факторам на рабочих местах. – М.: Изд-во стандартов, 2016. – 72 с.

8. СанПин 2.2.2.542-96. Гигиенические требования к видеодисплейным терминалам, персональным электронно-вычислительным машинам и организации работы. – М.: Изд-во стандартов, 1996. – 11 с.

9. ГОСТ Р 12.1.019-2009. Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты. – М.: Изд-во стандартов, 2010. – 32 с. «ССБТ. Электробезопасность. Общие требования и номенклатура видов защиты» [9].

10. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2008–02–01. – М.: Госстандарт России, 2001. – 12 с.

11. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – М.: Изд-во стандартов, 2009. – 40 с.

12. «Стратегия национальной безопасности Российской Федерации до 2020 года»: утверждена Указом Президента Российской Федерации от 12.05.2009 №

537: // КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

13. «Стратегия развития информационного общества»: утверждена Указом Президента от 07.02.2008 № Пр-212: // КонсультантПлюс. Технология 3000: Версия Проф [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

14. Федеральный закон «Об информации, информационных технологиях и защите информации»: федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ: // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.

15. ФГОС ВПО по направлению подготовки 090900 «Информационная безопасность». – Министерства образования и науки Российской Федерации, 2009. – 21с.

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ
Руководитель ГБУ «Инновационный бизнес-инкубатор»
_____
«____» _____ 2017 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
на объект информатизации
ИСПДн «Сотрудники и резиденты»

Государственное бюджетное учереждение «Инновационный бизнес-инкубатор»

СОСТАВИЛ

_____ И. А. Каретников

«____» _____ 2017 г.

2017 г.

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОБЪЕКТЕ

Наименование объекта: АС «Сотрудники и резиденты» государственного бюджетного учереждения «Инновационный бизнес-инкубатор».

Расположение объекта: Челябинская обл., г. Челябинск, ул. Троицкая, 1В, 2 этаж, кабинет № 201.

2 СОСТАВ ОБОРУДОВАНИЯ ОБЪЕКТА

Состав основных технических средств и систем (ОТСС) объекта информатизации отражен в таблице 2.1.

Таблица 2.1 – Перечень ОТСС, входящих в состав ОИ АС «Сотрудники и резиденты»

Наименование устройства	Фирма производитель, модель	Заводской / инвентаризационный номер	Расположение
Системный блок	Zalman Z3	ZZ14221096153	Рисунок 2.1
НЖМД	Seagate ST2000VM003	ST-0F54H274112	Рисунок 2.1
Монитор	Acer G236HLBbid	G21986lA1819289	Рисунок 2.1
Клавиатура	Logitech Keyboard K120	LK21KS5214AH	Рисунок 2.1
Мышь	Oklick 205M	OM93751621A5	Рисунок 2.1
Принтер	HP LaserJet M1522NF	XP21864041FD	Рисунок 2.1
ИБП	APC by Schneider Electric Back-UPS 500	AS261BU43CK	Рисунок 2.1

2.1 Состав вспомогательных технических средств и систем (ВТСС) объекта, установленных в помещении объекта информатизации отражен в таблице 2.2.

Таблица 2.2 – Перечень ВТСС ОИ АС «Сотрудники и резиденты»

Наименование устройства	Фирма производитель, модель	Заводской / инвентаризационный номер	Расположение
Системный блок	Zalman Z3	ZZ53F101A9	Рисунок 2.2
Монитор	Acer G236HLBbid	AG185201GJ	Рисунок 2.2
Клавиатура	Logitech Keyboard K120	LK391B84	Рисунок 2.2
Мышь	Oklick 205M	OK21K2912K	Рисунок 2.2
Системный блок	Zalman Z3	ZZ53B261C6	Рисунок 2.2
Монитор	Acer G236HLBbid	BEJE2241SX	Рисунок 2.2
Клавиатура	Logitech Keyboard K120	LK14A64K	Рисунок 2.2
Мышь	Oklick 205M	OK21K6932A	Рисунок 2.2
МФУ	Xerox Phaser 3260DNI	XP306125D	Рисунок 2.2
Телефонный аппарат	Panasonic KX-TS2388RU	PK216S8TS	Рисунок 2.2
Телефонный аппарат	Panasonic KX-TS2365RU	PKT216S4B	Рисунок 2.2
Телефонный аппарат	Panasonic KX-TS2365RU	PKV366S7B	Рисунок 2.2
Роутер	TP-LINK TL-WR841N	TP30519	Рисунок 2.2
Датчик пожарной сигнализации	б/н		Рисунок 2.2
Датчик пожарной сигнализации	б/н		Рисунок 2.2
Коммутатор	D-link DES-1008D/K3	DL125OF2157	Рисунок 2.2

Схема размещения и расположения ОТСС на объекте с привязкой к границам контролируемой зоны.

Структура, топология и размещение ОТСС и ВТСС объекта относительно границ контролируемой зоны объекта приведены на рисунках 2.1 – 2.3.

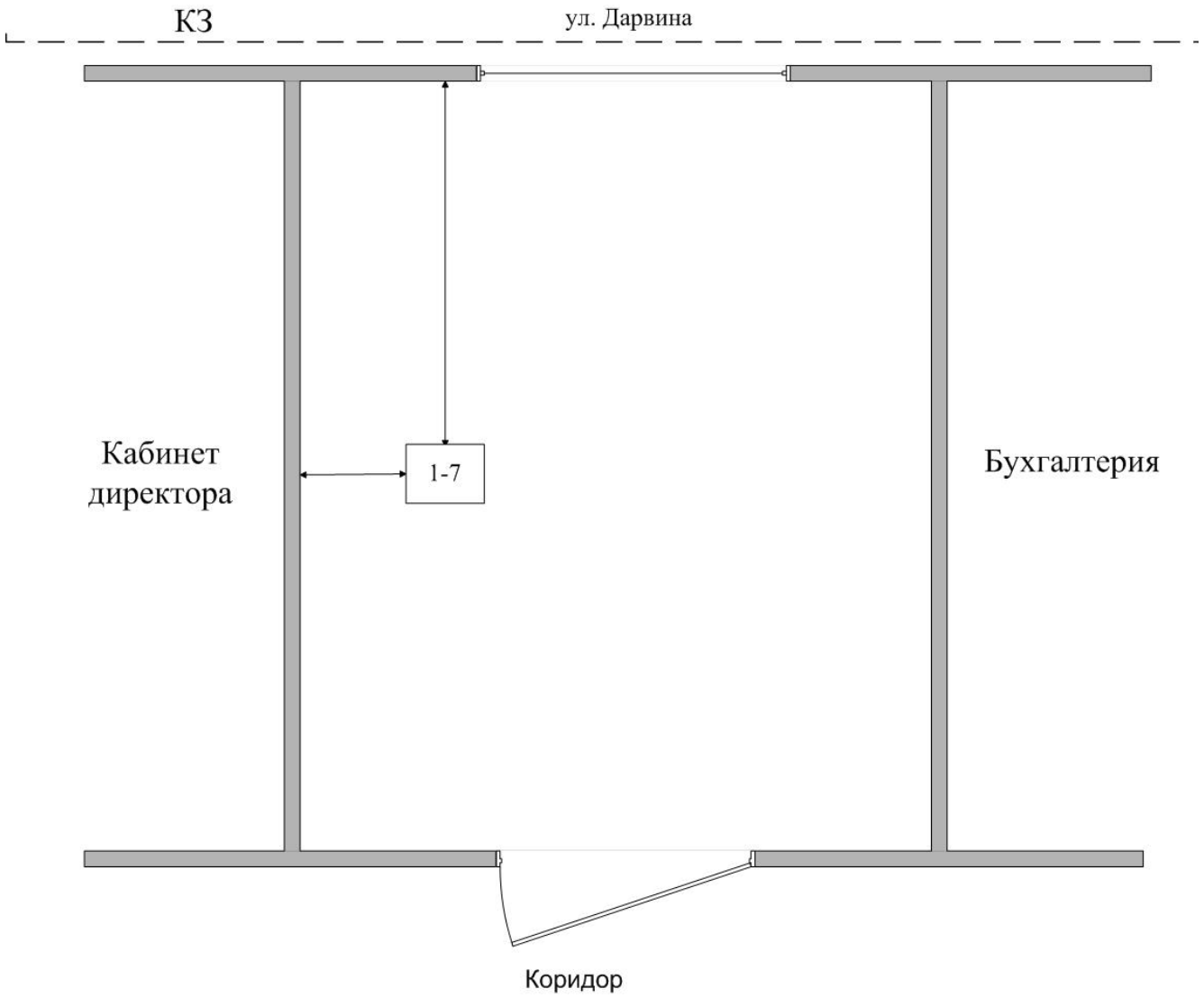


Рисунок 2.1 – Размещение ОТСС АС «Сотрудники и резиденты»

*Примечание: Обозначения 1-7 приведены в таблице 2.1 основной части технического паспорта.

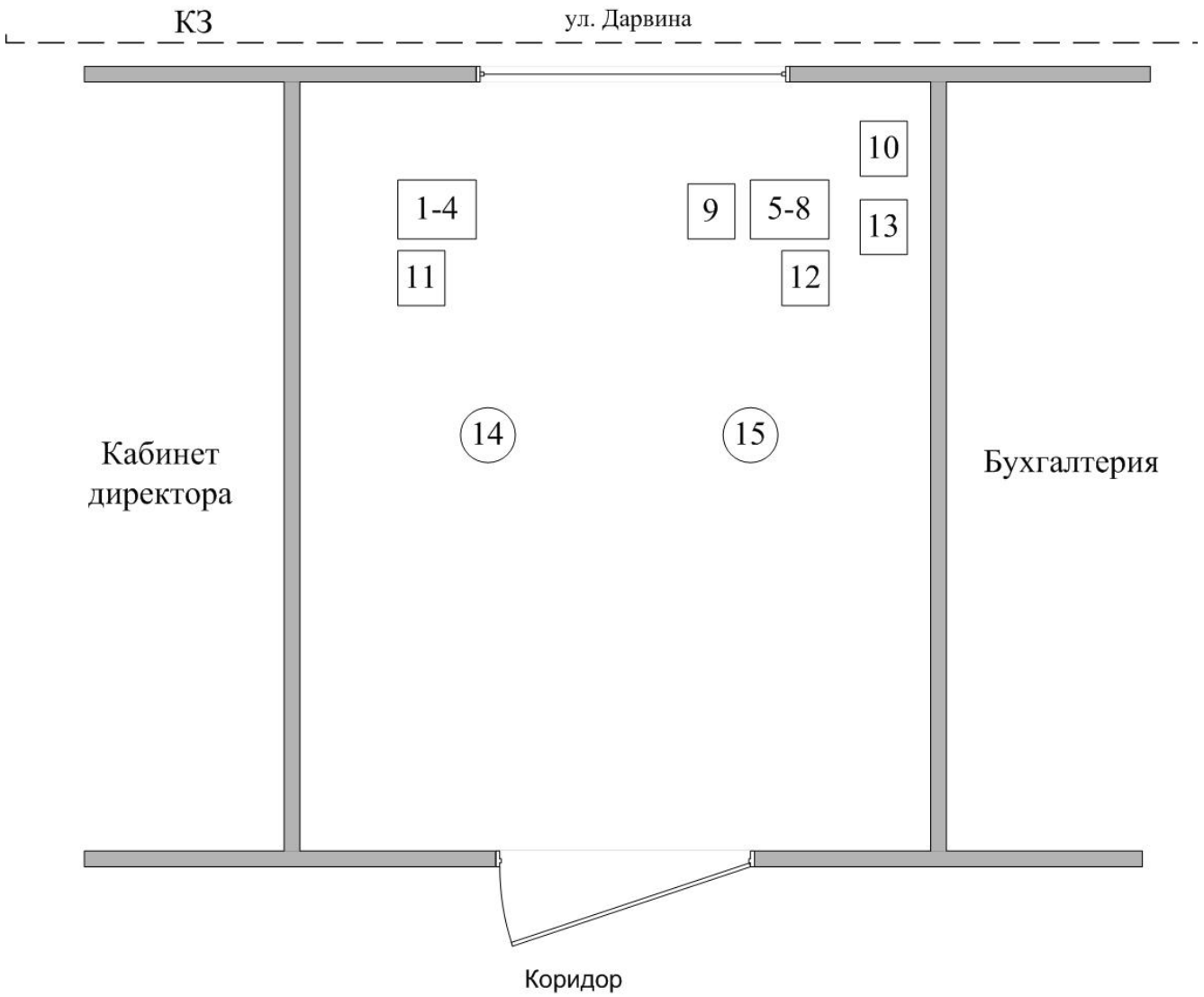
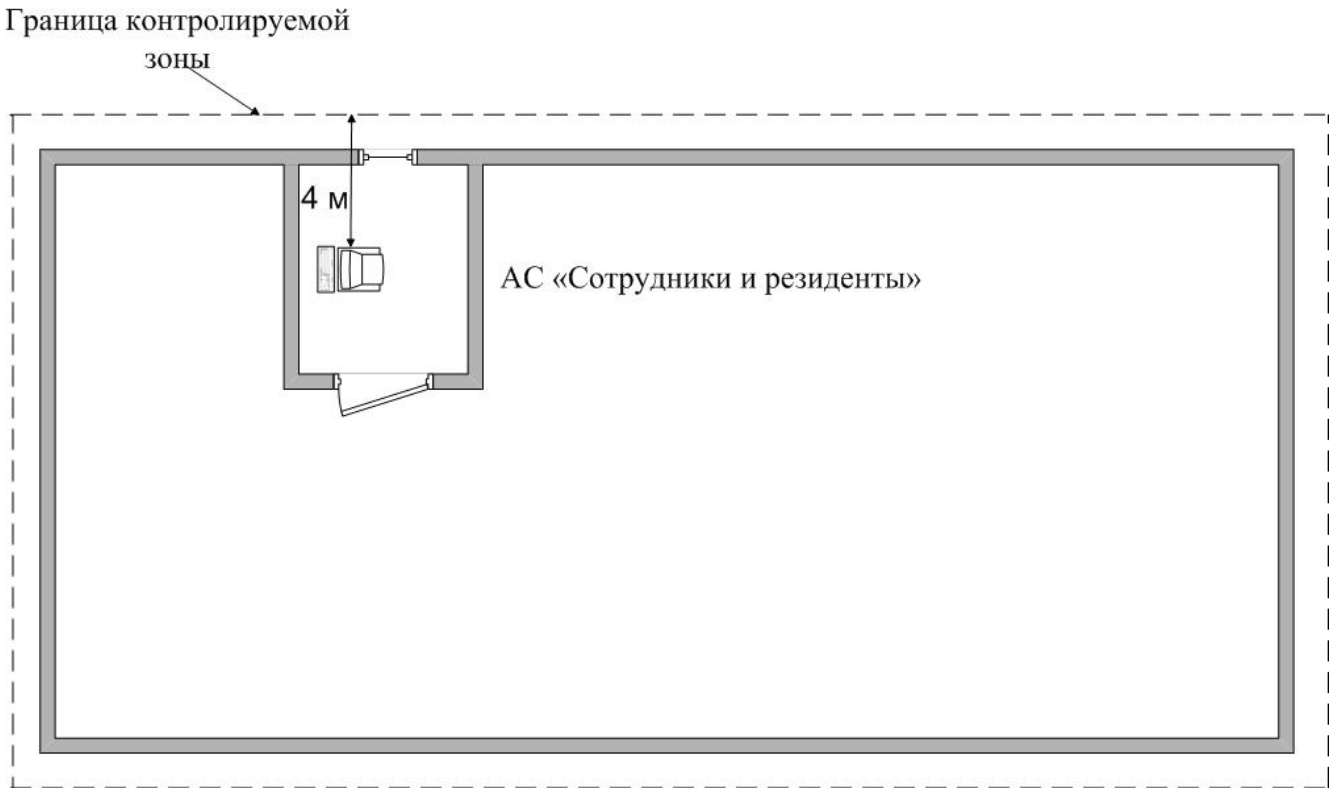


Рисунок 2.2 – Размещение ВТСС АС «Сотрудники и резиденты»

*Примечание: Обозначения 1-15 приведены в таблице 2.2 основной части технического паспорта.



2 этаж ГБУ «Инновационный бизнес-инкубатор», Челябинская обл., г. Челябинск, ул. Троицкая, д. 1в.

Рисунок 2.3 – Размещение ОТСС относительно границ контролируемой зоны

Границами контролируемой зоны является ограждающие конструкции здания государственного бюджетного учреждения «Инновационный бизнес-инкубатор», расположенное по адресу Челябинская обл., г. Челябинск, ул. Троицкая, д. 1в., согласно приказу «Об определении границ контролируемой зоны объекта информатизации АС "Сотрудники и резиденты» № 88 от 02.02.2018 г.

Кабинет расположен на втором этаже. Окно выходит на ул. Дарвина, на окнах висят жалюзи. Минимальное расстояние от ОТСС до КЗ составляет 4 метра.

2.4 Размещение линий ВТСС приведено на рисунке 2.4.

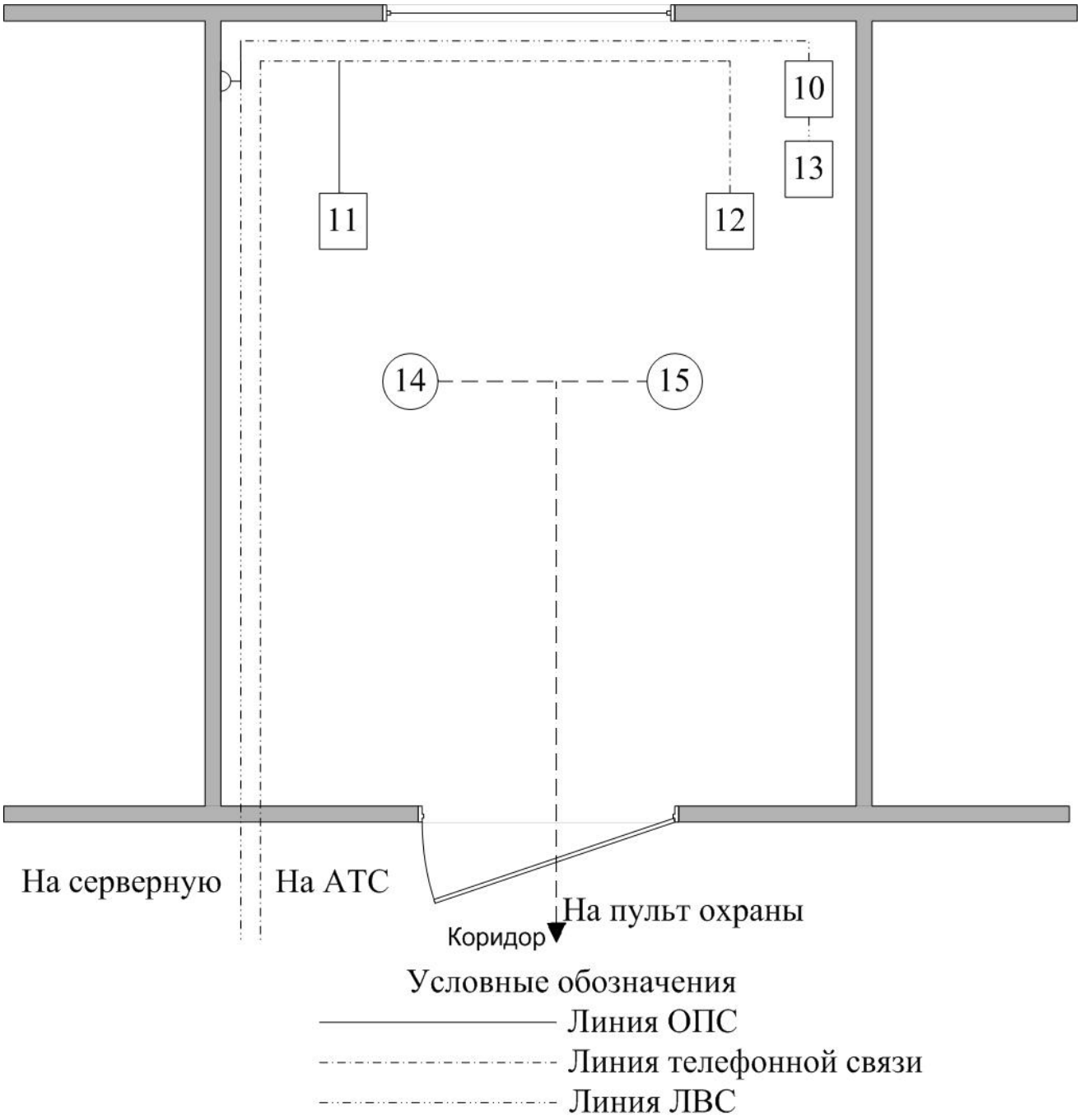


Рисунок 2.4 – Размещение ВТСС, расположение линий

*Примечание: Обозначения 11-15 приведены в Таблице 2.2 основной части технического паспорта

2.5 Размещение системы электропитания, заземления и инженерных коммуникаций приведено на рисунке 2.5.

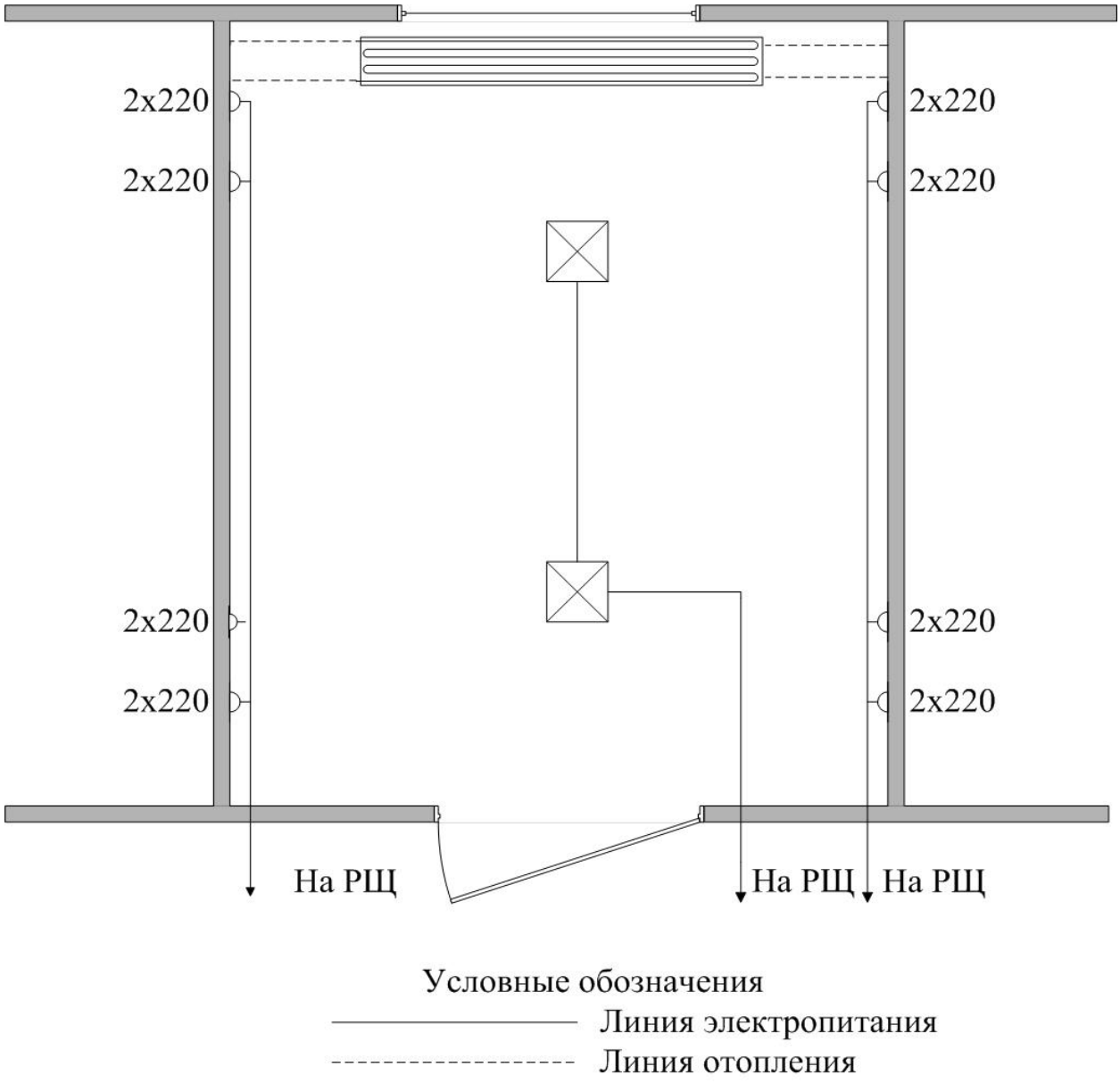


Рисунок 2.5 – Размещение системы электропитания, заземления и инженерных коммуникаций

Наименование линии	Выходит за пределы КЗ (выходит/не выходит)
Линия электропитания	не выходит
Линия заземления	не выходит
Линия охранной сигнализации	не выходит
Линия пожарной сигнализации	не выходит
Линия телефонной связи	выходит
Линия ЛВС	выходит
Линия отопления	выходит
Линия вентиляции	не выходит

2.6 Перечень средств защиты информации, установленных на объекте информатизации АС «Сотрудники и резиденты» приведен в Таблице 2.3.

Таблица 2.3 – Перечень средств защиты, установленных на ОИ АС «Сотрудники и резиденты»

Наименование и тип технического средства	Заводской номер/СЗЗ	Сведения о сертификате	Расположение
СЗИ от НСД «Secret Net 7»		№ 2707 действ. до 07.09.2018 г.	В ПЭВМ
Антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»		№ 3025 действ. до 25.11.2019 г.	В ПЭВМ
Межсетевой экран «TrustAccess»		№ 2146 действ. до 30.07.2019 г.	В ПЭВМ

2.7 Перечень программных средств, установленных на объекте информатизации АС «Сотрудники и резиденты» приведен в Таблице 2.4.

Таблица 2.4 – Перечень ПО установленного на ОИ АС «Сотрудники и резиденты»

Наименование ПО	Версия
Microsoft Windows 7 Professional SP1	6.1.7601.17514
Microsoft office 2016	2016
Secret Net 7	7
Kaspersky Endpoint Security 10 для Windows	10.2.5.3201
КриптоПро CSP	3.9.8171
TrustAccess	1.3

3 СВЕДЕНИЯ ОБ АТТЕСТАЦИИ ОБЪЕКТА ИНФОРМАТИЗАЦИ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО БЕЗОПАСНОСТИ ИНФОРМАЦИИ

3.1 Протоколы испытаний и даты их регистрации

3.2 Сведения об аттестации объекта информатизации на соответствие требованиям по безопасности информации:

Заключение по результатам аттестационных испытаний объекта информатизации №

Аттестат соответствия №

4 УЧЕТ ПРОВЕДЕНИЯ РЕГЛАМЕНТНЫХ ПРОВЕРОК

Таблица 4.1 –Учет проведения регламентных проверок

Наименование организации, проводившей проверку	Дата проведения проверки	Номер протокола	Примечание

5 ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Таблица 5.1 –Лист регистрации изменения состава и размещения ОТСС, ВТСС и средств защиты объекта информатизации

Дата внесения изменений	Наименование документа, фиксирующего изменения	Номера замененных (исправленных) листов формуляра	Подпись лица, внесшего изменения

ПРИЛОЖЕНИЕ Б

«УТВЕРЖДАЮ»
Руководитель
ГБУ «Инновационный бизнес-инкубатор»
А.А. Комарова
«___» _____2017 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на организацию защиты ИСПДн в ГБУ
«Инновационный бизнес-инкубатор»

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

Полное наименование системы: Организация системы защиты информационной системы обработки персональных данных «Сотрудники и резиденты», в государственном бюджетном учреждении «Инновационный бизнес-инкубатор».

Условное обозначение системы: организация системы защиты ИСПДН «Сотрудники и резиденты» в ГБУ «Инновационный бизнес-инкубатор».

1.2 Наименование заказчика и исполнителя

Предприятие разработчик системы: ГБУ «Инновационный бизнес-инкубатор», в лице главного специалиста по защите информации.

Предприятие заказчик системы: ГБУ «Инновационный бизнес-инкубатор», в лице генерального директора.

Перечень документов, на основании которых создается система:

- Конституция Российской Федерации;
- Федеральный закон от 27 июля 2007 года N 152-ФЗ «О персональных данных»
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Трудовой кодекс РФ от 30.12.2001 N 197-ФЗ;
- Порядок оформления и предъявления заказчику результатов работ по совершенствования системы (ее частей), по изготовлению и наладке отдельных средств (технических, программных, информационных) и программно-технических (программно-методических) комплексов системы
- Результаты работы оформляются и предъявляются заказчику по мере исполнения в виде минимальных независимых частей проекта и/или предварительных проектов. Окончательный вариант проекта предоставляется на рассмотрение заказчику после главного специалиста по защите информации ГБУ «Инновационный бизнес-инкубатор».

2. НАЗНАЧЕНИЕ И ЦЕЛИ ОРГАНИЗАЦИИ СИСТЕМЫ

2.1 Назначение организации системы

В связи с появлением новых производственных процессов в ГБУ «Инновационный бизнес-инкубатор», появилась необходимость в создании информационной системы персональных данных и её защите в соответствии с текущим законодательством.

2.2. Цели совершенствования системы

Основной целью проведения работ является приведение всех этапов работы с информации в информационной системе обработки персональных данных ГБУ «Инновационный бизнес-инкубатор» в соответствие требованиям перечисленных в данном Техническом задании.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

Объектом защиты является информационная система обработки персональных данных, представляющая из себя автоматизированное рабочее место, носителей информации ограниченного доступа, помещение, в котором расположена автоматизированная система:

1. Автоматизированные рабочие места:
- АРМ АС «Сотрудники и резиденты».
2. Помещения для хранения и работы с важной защищаемой информацией:
- Кабинет менеджеров.
3. Линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации:
- Линии проводной городской телефонной связи;
- Система электропитания;
- Линии охранной и пожарной сигнализации;
- Линии локальной компьютерной сети.
4. Средства ввода-вывода и отображения информации:
- Монитор;
- Принтер HP LaserJet 1018;
- Оперативная память ПК, входящего в АРМ.
5. Система бесперебойного питания АРМ:
- Источник бесперебойного питания АРМ главного бухгалтера.
6. Носители информации:
- Бумажные носители информации ограниченного доступа;
- Электронные (CD/DVD диски, флэш-накопители с документами, содержащими информацию ограниченного доступа);
- Персонал.
7. Персонал:
- Руководитель;
- Старший менеджер.

3.2. Сведения об условиях эксплуатации объекта защиты и характеристиках окружающей информационной среды

3.2.1. Объекты защиты подвержены воздействию следующих угроз:

3.2.1.1. АРМ старшего менеджера:

- Уничтожение информации в случае повреждения носителей информации;
- Несанкционированный доступ к информации в системе, хранящейся на АРМ главного менеджера.

3.2.2. Присутствуют следующие уязвимости:

АРМ главного менеджера: Отсутствие инструкции по эксплуатации СЗИ; Отсутствие описания технического процесса обработки информации ограниченного доступа; Отсутствие актов категорирования и классификации объекта информатизации.

4. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ ИСПДн «Сотрудники и резиденты» в ГБУ «Инновационный бизнес-инкубатор»

Работы должны проводиться в соответствии с положениями, перечисленными в данном Техническом задании.

Работы должны проводиться в два этапа:

- Приведение в соответствие с нормативно-правовыми актами порядка обработки персональных данных,
- проверка технических средств обработки информации;

4.1. Приведение в соответствие с нормативно-правовыми актами порядка обработки персональных данных

Список необходимых к проведению работ относительно информационной системы обработки персональных данных:

- Разработка нормативно-правовой документации: Акта обследования АС, акта классификации АС, описания технологического процесса обработки информации, инструкции по эксплуатации СЗИ, технического паспорта;
- Изучение существующих организационных мер обеспечения безопасности информации ограниченного доступа;
- Разработка актуализированной модели угроз;
- Разработка перечня требований по защите персональных данных;
- Выявление имеющихся средств технической защиты информации и мер, которые применяются для обеспечения безопасности персональных данных;
- Анализ соответствия применяющихся мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных.

4.2. Проверка технических средств обработки информации

- Список необходимых к проведению работ относительно информационной системы обработки персональных данных:
- Определение условий расположения технических средств обработки информации ограниченного доступа относительно границ контролируемой зоны;
- Определение линий и коммуникаций, расположенных в месте размещения технических средств обработки информации ограниченного доступа;
- Изучение существующих организационных мер обеспечения безопасности работоспособности и функционирования информационных систем;
- Покупка необходимых программных и технических средств, для обеспечения повышения защищенности информационной системы персональных данных;
- Обновление программных продуктов информационной системы до актуального состояния;

4.3. Порядок проведения работ:

3.3.1. Для выполнения работ Исполнитель привлекает специалистов Заказчика имеющих необходимую компетенцию.

4.3.2. Специалисты Заказчика временно переходят под руководство Исполнителя.

4.3.3.В ходе проведения работ Исполнитель собирает исходные данные путем:

- опроса персонала Заказчика, в том числе руководителей и сотрудников структурных подразделений;
- обследования АРМ и места его расположения;
- анализа документов и записей результатов деятельности Заказчика в части обеспечения безопасности информационных систем персональных данных (нормативных документов, проектной и эксплуатационной документации, актов, журналов и пр.).

5. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ СИСТЕМЫ ЗАЩИТЫ ИСПДн

5.1. Критериями для приемки работ является настоящее техническое задание и соответствующие частные Технические задания, разрабатываемые в процессе выполнения работ.

5.2. Приемка работ осуществляется единовременно.

5.3. Заказчик направляет замечания в письменном виде.

6. ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ ПРОЕКТА РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА ЗАЩИТЫ К ВВОДУ СИСТЕМЫ ЗАЩИТЫ ИСПНДн В ДЕЙСТВИЕ

При подготовке к проведению Исполнителем работ со стороны Заказчика необходимо обеспечить следующее:

- назначить ответственное лицо от Заказчика, наделенное соответствующими полномочиями, для обеспечения выполнения работ Исполнителем;
- определить лицо для организации и проведения опроса;
- обеспечить промежутки времени доступности лиц, АРМ и выделенного помещения.

7. ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

7.1. При разработке системы Исполнителем должны быть подготовлены следующие документы:

- Акт обследования автоматизированной системы;
- Технический паспорт.
- Акт классификации ИСПДн;
- Перечень персональных данных подлежащих защите;
- Модель угроз для ИСПДн;
- Описание технического процесса обработки персональных данных;

7.2. Отчетные документы предоставляются Заказчику в электронном виде в формате документов Microsoft Office и на бумажных носителях.

8. ДОПОЛНИТЕЛЬНЫЕ УСЛОВИЯ И ОГРАНИЧЕНИЯ

8.1. В случае поставки и внедрения технических средств защиты третьей стороной до начала работ по аттестации, Заказчик согласует с Исполнителем следующее:

- состав и спецификацию технических средств;
- состав сопроводительной документации к техническим средствам и сертификатов;
- схемы установки и подключения;
- настройки аппаратно-программных средств;
- рабочую документацию этапа внедрения.

8.2. Срок поставки и внедрения технических средств защиты не входит в расчет сроков этапов работ.

В случае задержки по срокам предоставления исходных данных при проведении работ, или неполного предоставления информации со стороны Заказчика, по согласованию сторон возможен перенос сроков выполнения работ по договору в сторону увеличения.

ПРИЛОЖЕНИЕ В

УТВЕРЖДАЮ
Руководитель ГБУ «Инновационный бизнес-инкубатор»
_____А.А. Комарова
«____»_____2017 г.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ,
подлежащих защите в информационной системе обработки персональных данных «Сотрудники и резиденты»

№	Тип персональных данных, подлежащих защите
1.	Фамилия, Имя, Отчество
2.	Паспортные данные
3.	Дата рождения
4.	Адреса проживания и прописки
5.	Сведения об образовании
6.	Учебное заведение
7.	Образовательное заведение
8.	Индивидуальный номер налогоплательщика
9.	Основной государственный регистрационный номер
10.	Страховой номер индивидуального лицевого счета

Руководитель
ГБУ «Инновационный бизнес-инкубатор» _____ А.А. Комарова

ПРИЛОЖЕНИЕ Г

Для построения диаграммы Ганта определим перечень поставленных задач и их сроки (с учетом выходных дней).

Название работы	Длительность	Начало	Окончание
1. Проектирование	12	02.02.2017	14.02.2017
1.1. Изучение существующих организационных мер обеспечения безопасности персональных данных	3	02.02.2017	02.05.2017
1.2. Разработка частной модели угроз	3	05.02.2017	08.02.2017
1.3. Категорирование и определение уровня защищенности ИСПДн	3	08.02.2017	11.02.2017
1.4. Анализ соответствия применяющихся мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных	3	11.02.2017	14.02.2017
2. Стадия проектирования	17	14.02.2017	03.03.2017
2.1. Разработка организационно-распорядительной документации	7	14.02.2017	21.02.2017
2.2. Приобретение СЗИ от НСД	5	21.02.2017	26.02.2017
2.3. Приобретение межсетевого экрана	5	26.02.2017	03.03.2017
3. Реализация системы защиты ИСПДн;	14	03.03.2017	17.03.2017
3.1. Установка и настройка СЗИ от НСД	3	03.03.2017	06.03.2017
3.2. Установка и настройка антивирусного ПО	3	06.03.2017	09.03.2017
3.3. Обучение пользователей	4	09.03.2017	13.03.2017
3.4. Контроль защищенности	4	13.03.2017	14.03.2017

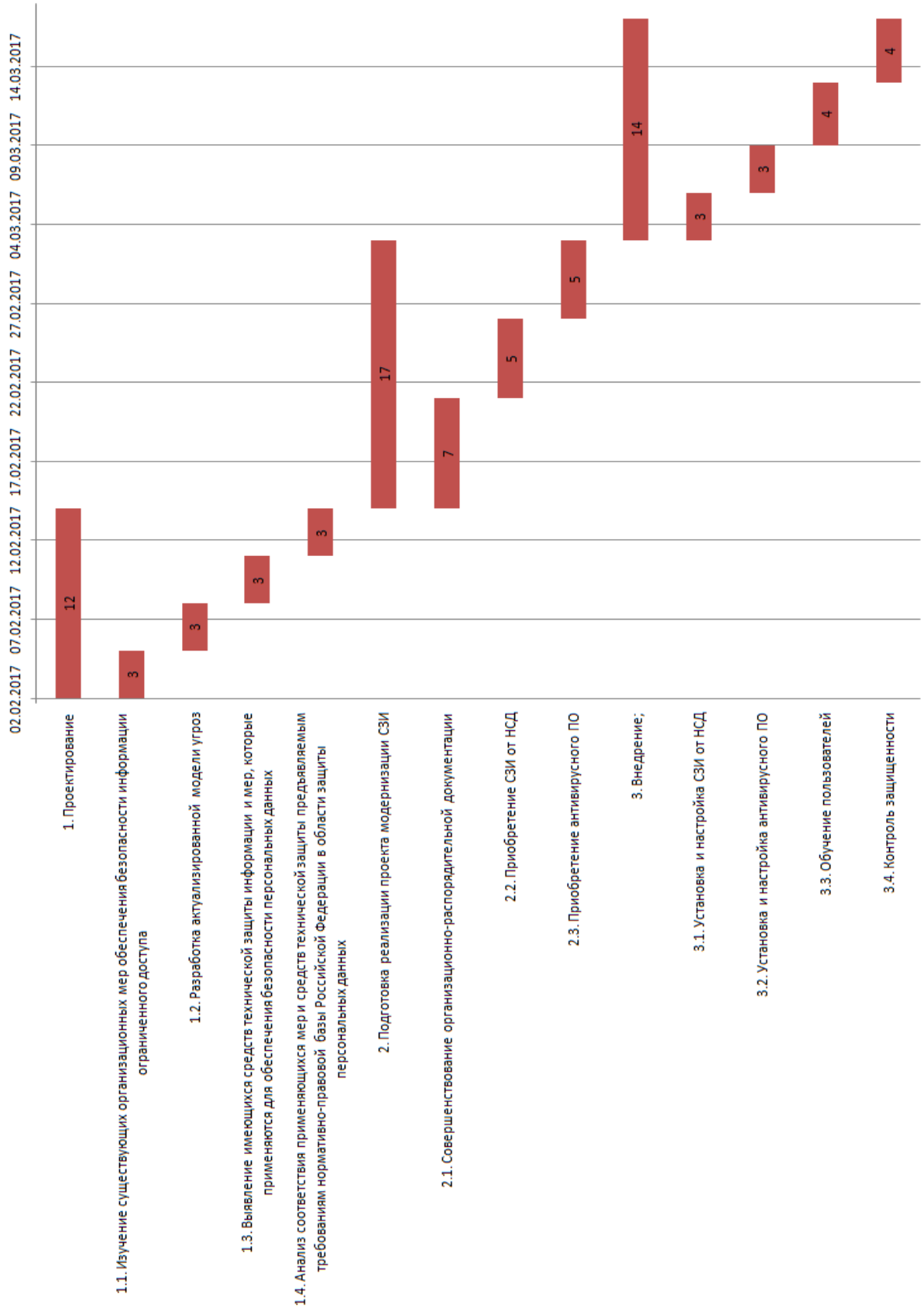


Рисунок 1.1 – Диаграмма Ганта

ПРИЛОЖЕНИЕ Д

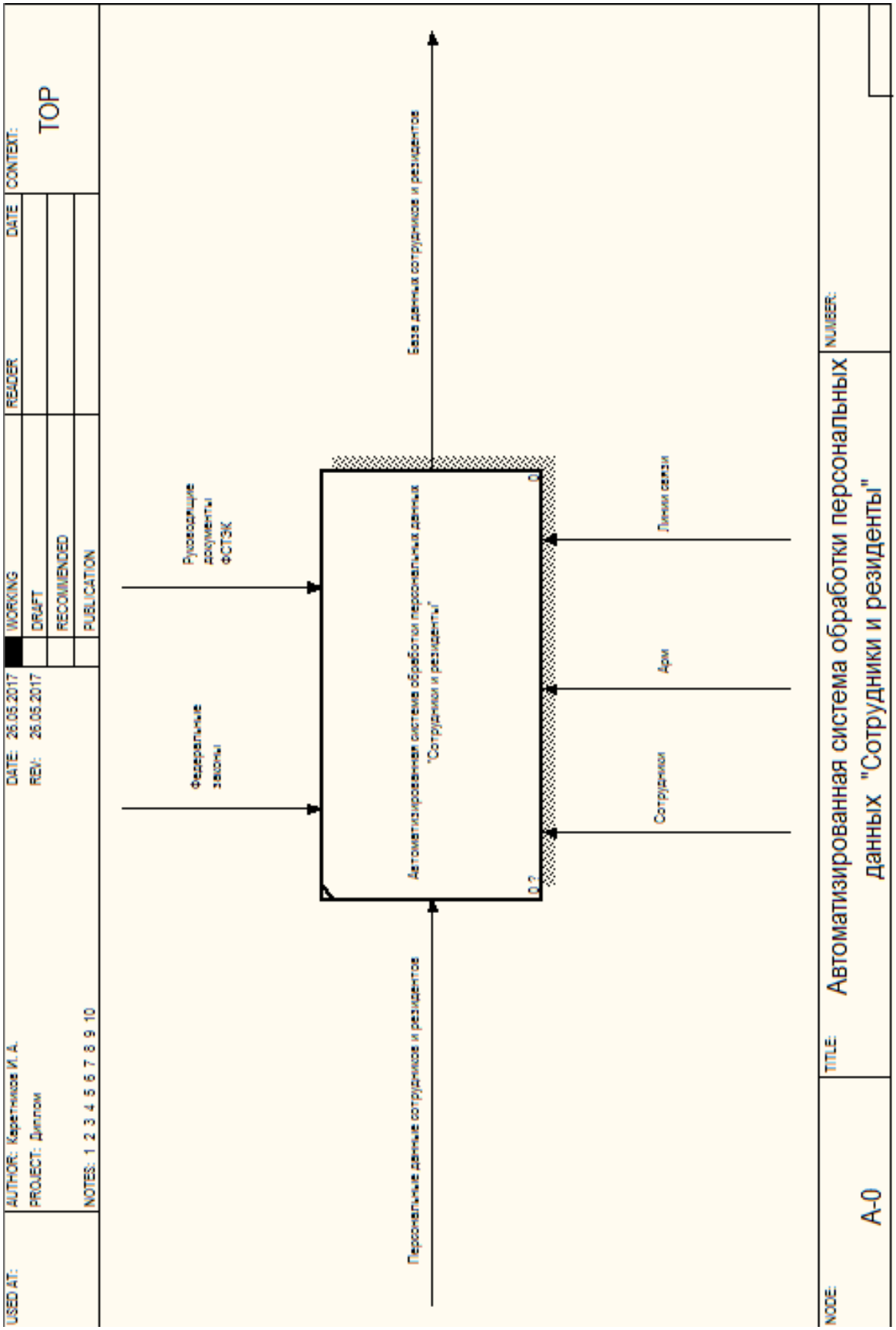
Для своевременного выполнения работ, а также соответствия плану работ необходимо определить сроки выполнения работ (Таблица 1).

i-j – код работы
T – длительность работы, дней
$T_{рн}$ – ранний срок начала работы
$T_{пн}$ – поздний срок начала работы
$T_{ро}$ – ранний срок окончания работы
$T_{по}$ – поздний срок окончания работы

Таблица 1– Расписание выполнения работ

i-j	Название работы	T	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
	Проектирование	12	0	0	12	12
1-2	Изучение существующих организационных мер обеспечения безопасности персональных данных	3	0	0	3	3
2-3	Разработка частной модели угроз	3	3	3	6	6
3-4	Категорирование и определение уровня защищенности ИСПДн	3	6	6	9	9
4-5	Анализ соответствия применяющихся мер и средств технической защиты предъявляемым требованиям нормативно-правовой базы Российской Федерации в области защиты персональных данных	3	9	9	12	12
	Стадия проектирования	17	12	12	29	29
6-7	Разработка организационно-распорядительной документации	7	12	12	19	19
7-8	Приобретение СЗИ от НСД	5	19	19	24	24
8-9	Приобретение межсетевого экрана	5	24	24	29	29
	Реализация системы защиты ИСПДн;	14	29	29	43	43
9-10	Установка и настройка СЗИ от НСД	3	29	29	32	32
10-11	Установка и настройка антивирусного ПО	3	32	32	35	35
11-12	Обучение пользователей	4	35	35	39	39
12-13	Контроль защищенности	4	39	39	43	43

ПРИЛОЖЕНИЕ Е



ПРИЛОЖЕНИЕ Ж

УТВЕРЖДАЮ
Руководитель ГБУ «Инновационный бизнес-инкубатор»
_____ А.А. Комарова
«_____»_____ 2017 г.

АКТ

Определение уровня защищенности персональных данных при их обработке в информационной системе «Сотрудники и резиденты» в ГБУ «Инновационный бизнес-инкубатор»

Комиссия, назначенная приказом руководителя «Инновационный бизнес-инкубатор» от 02.02.2017 № 87 в составе:

Председатель:
Руководитель ГБУ «Инновационный бизнес-инкубатор» Комарова А.А.
Члены комиссии:
Специалист по информационной безопасности
Главный инженер ГБУ «Инновационный бизнес-инкубатор» Замятин С.Б.
Старший системный администратор ГБУ «Инновационный бизнес-инкубатор» Кокин И.Е.

Рассмотрев исходные данные об информационной системе, в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» установила:

1) информационная система является информационной системой, обрабатывающей **иные категории персональных данных субъектов персональных данных, не являющихся сотрудниками оператора;**

2) объем обрабатываемых персональных данных: **менее 100 000 субъектов ПДн**;

3) в соответствии с моделью угроз в информационной системе актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе: **актуальны угрозы 3-го типа.**

В соответствии с пунктом 12 «Требований к защите персональных данных при их обработке в информационных системах персональных данных», утвержденных постановлением Правительства Российской Федерации от 01.11.2012 № 1119 и на основании анализа исходных данных, комиссия:

Решила:

в информационной системе персональных данных «Сотрудники и резиденты» ГБУ «Инновационный бизнес-инкубатор» присвоить: **4 уровень защищенности персональных данных.**

Председатель комиссии:

_____ Комарова А.А.

Члены комиссии:

_____ Замятин С.Б.

_____ Кокин И.Е.

«02» февраля 2017 г

ПРИЛОЖЕНИЕ З

ЧАСТНАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ИСПДн «Сотрудники и резиденты»

Угроза	Исходная защищенность (Y1)	Частота реализации угрозы (Y2)	Коэффициент реализуемость угрозы (Y)	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
1. Угрозы несанкционированного доступа к информации						
1.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн						
1.1.1. Кража ПЭВМ	5	маловероятна	0,25	низкая	низкая	неактуальная
1.1.2. Кража носителей информации	5	маловероятна	0,25	низкая	низкая	неактуальная
1.1.3. Кража ключей и атрибутов доступа	5	маловероятна	0,25	низкая	низкая	неактуальная
1.1.4. Кража, модификация, уничтожение информации	5	маловероятна	0,25	низкая	низкая	неактуальная
1.1.5. Вывод из строя узлов ПЭВМ, каналов связи	5	маловероятна	0,25	низкая	низкая	неактуальная
1.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	5	маловероятна	0,25	низкая	низкая	неактуальная
1.1.7. Несанкционированное отключение средств защиты	5	низкая вероятность	0,35	средняя	низкая	неактуальная
1.2.1.Угрозы хищения, несанкционированной модификации или блокирования информации за счет несанкционированного доступа (НСД) с применением программно-аппаратных и программных средств (в том числе программно-математических воздействий)						
1.2.1.1. Действия вредоносных программ (вирусов)	5	высокая вероятность	0,75	высокая	низкая	актуальная
1.2.1.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	5	маловероятна	0,25	низкая	низкая	неактуальная
1.2.1.3. Установка ПО, не связанного с исполнением служебных обязанностей	5	средняя вероятность	0,5	средняя	низкая	неактуальная
1.2.2. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из-за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п) характера						
1.2.2.1. Утрата ключей и атрибутов доступа	5	средняя вероятность	0,5	средняя	низкая	неактуальная
1.2.2.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	5	высокая вероятность	0,75	высокая	низкая	актуальная
1.2.2.3. Непреднамеренное отключение средств защиты	5	высокая вероятность	0,75	высокая	низкая	актуальная
1.2.2.4. Выход из строя аппаратно-программных средств	5	средняя вероятность	0,5	средняя	низкая	неактуальная
1.2.2.5. Сбой системы электроснабжения	5	маловероятна	0,25	низкая	низкая	неактуальная
1.2.2.6. Стихийное бедствие	5	маловероятна	0,25	низкая	низкая	неактуальная

Угроза	Исходная защищенность (Y1)	Частота реализации угрозы (Y2)	Коэффициент реализуемость угрозы (Y)	Возможность реализации угрозы	Показатель опасности угрозы	Актуальность угрозы
2. Угрозы преднамеренных действий внутренних нарушителей						
2.1. Доступ к информации, модификация, уничтожение лицами, не до-пущенными к ее обработке						
2.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	5	высокая вероятность	0,75	высокая	низкая	актуальная
3. Угрозы несанкционированного доступа по каналам связи						
3.1. Угроза «Анализ сетевого траффика»	5	маловероятна	0,25	низкая	низкая	неактуальная
3.2. Угроза «сканирование сети»	5	высокая вероятность	0,75	высокая	низкая	актуальная
3.3. Угроза выявления паролей	5	маловероятна	0,25	низкая	низкая	неактуальная
3.4. Угрозы навязывания ложного маршрута сети	5	маловероятна	0,25	низкая	низкая	неактуальная
3.5. Угрозы подмены доверенного объекта	5	маловероятна	0,25	низкая	низкая	неактуальная
3.6. Внедрение ложного объекта сети	5	маловероятна	0,25	низкая	низкая	неактуальная
3.7. Угрозы типа «Отказ в обслуживании»	5	высокая вероятность	0,75	высокая	низкая	актуальная
3.8. Угрозы удаленного запуска приложений	5	маловероятна	0,25	низкая	низкая	неактуальная
3.9. Угрозы внедрения по сети вредоносных программ	5	средняя вероятность	0,35	средняя	низкая	неактуальная

ПРИЛОЖЕНИЕ И

ПРИКАЗ
№ 89 от « » _____ 2017 г.

Об организации работ по обеспечению безопасности персональных данных в ГБУ «Инновационный бизнес-инкубатор»

В целях обеспечения безопасности персональных данных при их обработке в ИСПДн «Сотрудники и резиденты» ГБУ «Инновационный бизнес-инкубатор», в соответствии с Федеральным законом от 27.07.2006 №152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», приказом Федеральной службы по техническому и экспортному контролю от 18.02.2013 №21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» п р и к а з ы в а ю:

Назначить ответственным за организацию обработки персональных данных в информационных системах персональных данных ГБУ «Инновационный бизнес-инкубатор»

Старшего системного администратора Кокина И.Е.

Утвердить «Инструкцию ответственного лица за обработку персональных данных в ГБУ «Инновационный бизнес-инкубатор»

Возложить на Кокина И.Е. следующие обязанности:

- предоставление на утверждение списка лиц, доступ которых к персональным данным, обрабатываемым в информационных системах персональных данных ГБУ «Инновационный бизнес-инкубатор»

необходим для выполнения служебных (трудовых) обязанностей, а также изменений к нему;

- осуществление внутреннего контроля за соблюдением работниками ГБУ «Инновационный бизнес-инкубатор»

законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;

- доведение до сведения работников (оператора) положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организация приема и обработка обращений субъектов персональных данных или их представителей и осуществление контроля за приемом и обработкой таких обращений.

4. Контроль за исполнением настоящего приказа оставляю за собой.

Руководитель ГБУ «Инновационный бизнес-инкубатор» _____ Комарова А.А.