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»

РАБОТА ПРОВЕРЕНА
Рецензент,
Руководитель доп. офиса №5 АО
«УРАЛПРОМБАНК»
_____ В.Э. Гогель
_____ 2018 г.

ДОПУСТИТЬ К ЗАЩИТЕ
Заведующий кафедрой,
к.т.н., доцент
_____ А.Н. Соколов
_____ 2018 г.

Защита информационной системы персональных данных на предприятии АО «УРАЛПРОМБАНК»

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ
ЮУрГУ – 10.05.03.2018.267.ПЗ ВКР

Консультанты

Безопасность жизнедеятельности,
к.т.н., доцент
_____ Н.В. Глотова
_____ 2018 г.

Руководитель проекта,
зам. директора ООО
«Стратегия безопасности»
_____ Е.Ю. Мищенко
_____ 2018 г.

Автор проекта,
студент группы КЭ-530
_____ В.Д. Лопатин
_____ 2018 г.

Экономическая часть,
ст. преп.
_____С.А. Сабельников
_____ 2018 г.

Нормоконтролер,
к.т.н., доцент
_____ В.П. Мартынов
_____ 2018 г.

Челябинск 2018

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»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А.Н. Соколов

_____ 2018 г.

З А Д А Н И Е
на выпускную квалификационную работу студента

Лопатина Виталия Дмитриевича

Группа ___*КЭ-530*

1. Тема работы

Защита информационной системы персональных данных

АО «УРАЛПРОМБАНК»

Утверждена приказом ректора ЮУрГУ от _____ № _____
(утверждена, прот. заседания кафедры от _____ № _____)

2. Срок сдачи студентом законченной работы _____

3. Исходные данные к работе

Отчет о преддипломной практике, нормативно-правовые документы в области защиты информации, документация предприятия-базы практики

4.Содержание расчетно-пояснительной записки (перечень подлежащих разработке вопросов)

4.1 Анализ состояния информационной системы

4.2 Теоретическое обоснование выбора средств защиты

4.3 Разработка технического задания модернизации системы

5.Перечень графического материала (с точным указанием обязательных чертежей, плакатов в листах формата А1)

*Презентация «*Защита информационной системы персональных данных *АО «УРАЛПРОМБАНК» в формате PowerPoint 2010 (pptx)*

Количество слайдов -

Всего ___ листов

6. Консультанты по работе (проекту), с указанием относящихся к ним разделов работы (проекта)

Раздел	Консультант	Подпись, дата	
		Задание выдал (консультант)	Задание принял (студент)
Безопасность жизнедеятельности	Н.В. Глотова		

7. Дата выдачи задания _____

Руководитель,
ст.преп. _____ _____Е.Ю. Мищенко

Задание принял к исполнению _____В.Д. Лопатин

КАЛЕНДАРНЫЙ ПЛАН

Наименование этапов выпускной квалификационной работы (проекта)	**Срок выполнения этапов работы**	**Отметки о выполнении руководителя**
Введение		
1 Анализ состояния информационной системы		
2 Теоретическое обоснование выбора средств защиты		
3 Разработка технического задания модернизации системы		
4 Расчёт экономической эффективности		
5 Безопасность жизнедеятельности		
Заключение		
Библиографический список		
Предзащита ВКР		
Защита ВКР		

Заведующий кафедрой _____ А.Н. Соколов

Руководитель работы _____ Е.Ю. Мищенко

Студент _____ В.Ж. Лопатин

АННОТАЦИЯ

Лопатин В.Д. Защита информационной системы обработки персональных данных на предприятии АО «УРАЛПРОМБАНК» – Челябинск: ЮУрГУ, КЭ-530, __ с., _ ил., __ табл., библиогр. список – _ наим., _ прил.

Выпускная квалификационная работа выполнена с целью совершенствования системы защиты информационной системы обработки персональных данных в АО «УРАЛПРОМБАНК».

В выпускной квалификационной работе отражены все этапы модернизации системы защиты персональных данных, от сбора исходных данных до заключения о соответствии нормативным документам РФ по защите персональных данных.

Работа состоит из четырёх глав. В процессе выполнения квалификационной работы было проведено обследование предприятия, созданы все необходимые документы, регламентирующие порядок защиты информации, а также описывающих информационную систему персональных данных предприятия. Было проведено перепроектирование системы защиты, включающее в себя выбор средств защиты, предотвращающих актуальные угрозы банка, приведено обоснование их эффективности и экономической целесообразности.

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

АПКШ – аппаратно-программный комплекс шифрования;
АРМ – автоматизированное рабочие место;
ВТСС – вспомогательные технические средства и системы;
ЗИ – защита информации;
ИБ – информационная безопасность;
ИС – информационная система;
ИСПДн – информационная система персональных данных;
ИТ – информационные технологии;
МСЭ – межсетевой экран;
НСД – несанкционированный доступ;
АО – акционерное общество;
ОТСС – основные технические средства и системы;
ПАК – программно-аппаратный комплекс;
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;

Ресурс – любой контейнер, предназначенный для хранения информации, подверженный угрозам информационной безопасности (сервер, рабочая станция, переносной компьютер). Свойствами ресурса являются: перечень угроз, воздействующих на него, и критичность ресурса;

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

Обработка информации, на сегодняшний день, является одним из наиболее трудоемких процессов, особенно если эта информация ограниченного доступа. Скорость обработки информации и качество получаемых результатов, являются важными факторами, обеспечивающими конкурентоспособность фирмы, а результаты могут являться одним из важнейших активов организации.

Невозможно представить деятельность банка без обработки информации о людях. Обрабатываются данные о сотрудниках, клиентах, партнерах, акционеров и т.д. Вся эта информация является персональными данными. Постановлением Правительства РФ от 1 ноября 2012 г. № 1119 установлены требования к защите персональных данных при их обработке в информационных системах. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор этой системы или лицо, осуществляющее обработку персональных данных по поручению оператора на основании заключаемого с этим лицом договора. Выбор средств защиты информации для системы осуществляется оператором в соответствии с нормативными правовыми актами.

Актуальность данной работы обусловлена необходимостью модернизации системы защиты информационных систем обработки персональных данных в дополнительном офисе №5 АО «УРАЛПРОМБАНК» в связи с проектом, который предусматривает внесение фото клиентов в базу данных и добавление рабочего места.

Объектом выпускной квалификационной работы является филиал АО «УРАЛПРОМБАНК» в городе Коркино.

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

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

В соответствии с поставленной целью необходимо решить следующие задачи:

- проанализировать информационную систему АО «УРАЛПРОМБАНК», с целью обоснования необходимости модернизации системы защиты информационной системы обработки персональных данных;
- выявить защищаемую информацию;
- разработать модель угроз;
- провести анализ и теоретическое обоснование выбора средств защиты информации;
- разработать техническое задание по модернизации системы защиты информационной системы обработки персональных данных в АО «УРАЛПРОМБАНК»;
- внести изменения в существующие документы и, при необходимости составить новые.

1. АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В АО «УРАЛПРОМБАНК» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Разработка технического паспорта

Для модернизации системы защиты информации было проведено обследование предприятия с учётом нового рабочего места, в результате которого был составлен технический паспорт (Приложение А).

В техническом паспорте приведен состав АРМ схемы их размещения, перечень установленных средств защиты информации и программного обеспечения.

В качестве объекта защиты была выбрана ИСПДн «КЛИЕНТЫ БАНКА» дополнительного офиса №5 АО «УРАЛПРОМБАНК».

1.2. Выявление защищаемой информации

В результате проведенного обследования была выявлена следующая защищаемая информация: перечень персональных данных, подлежащих защите в информационной системе обработки персональных данных «КЛИЕНТЫ БАНКА».

В рамках данной ВКР был разработан перечень персональных данных (Приложение В).

1.3. Описание информационной системы

Система защиты информации в ИСПДн «КЛИЕНТЫ БАНКА» АО «УРАЛПРОМБАНК» основана на использовании организационных, правовых и программно-аппаратных мер.

Организационные меры включают в себя инструкции администратора, инструкции пользователей, инструкцию по эксплуатации СЗИ, инструкцию по антивирусной, инструкцию по парольной защите, инструкцию по резервированию, журнал учета лиц, журнал учета машинных носителей.

В рамках ВКР была разработана инструкция по антивирусной защите (Приложение Г) и инструкция по парольной защите(Приложение Е). Инструкции администратора, инструкции пользователей, инструкция по эксплуатации СЗИ, инструкция по резервированию, журнал учета лиц, журнал учета машинных носителей ранее существовали на предприятии.

Правовые меры включают в себя нормативно-правовые документы, регулирующие деятельность организации в области обеспечения защиты информации:

– базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) [1];

– методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных [6];

– Федеральный закон «О персональных данных» [15];

– Постановление Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [7];

– Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

Программно-аппаратные меры включают в себя программно-аппаратные средства, обеспечивающих работу информационной системы и ее защиту. В рамках ВКР была проведена инвентаризация информационной системы, результаты которой представлены в Таблицах 1 и 2.

Таблица 1 – Аппаратное обеспечение

Наименование устройства	Фирма производитель, модель	Заводской / инвентаризационный номер	Количество
Системный блок	HP260	a102urZ0J78EA	5
Твердотельный накопитель	WD WD3200AAKX-001CA0	WD-WCAYUAA20921	5
Монитор	LG L1942S-BF	907NDBP3G709	5
Клавиатура	Genius K639	ZM7902171374	5
Мышь	OKLICK 225M	0907	5
Принтер	HP LaserJet 1018	CNC1L86960	3
ИБП	APC SmartuPS 500	QS0614121487	5
Телефонный аппарат	Panasonic KX	TS2352	5
Коммутатор	Cisco 5510		1
Датчик пожарной сигнализации	б/н		5
Камера	Rekam A140	RE17137421	3
Камера	Falcon Eye	Eye FE-B720AHD	3
МФУ	HP LaserJet Pro	CNC1L251230	1
Пульт ОПС	б/н		1

Таблица 2 – Программное обеспечение

Наименование	Версия
Microsoft Windows 10	1703
7-zip	9.20.00.0
Kaspersky Endpoint Security 10 для Windows	10.2.5.3201
Операционный день банка	3.1
1С: Предприятие	8
1С: Бухгалтерия	
Microsoft office 365	

1.4. Выявление объектов защиты

Основываясь на перечне защищаемой информации, были выявлены объекты защиты и составлен их перечень:

- АРМ, на которых обрабатывается защищаемая информация;
- источники бесперебойного питания
- средства ввода-вывода и отображения информации;
- система бесперебойного питания АРМ;
- линии и средства связи, системы обеспечения функционирования СВТ и деятельности организации;
- носители информации;
- персонал.

Полный перечень объектов защиты представлен в Приложении А.

1.5. Разработка модели угроз

Модель угроз безопасности информации, учитывая особенности информационной системы, используемые в ней программные, программно-технические, технические средства и процессы обработки информации, дает описание угроз безопасности, которым подвержена информационная система.

На основании модели деятельности организации был сформулирован перечень важных объектов защиты:

- персонал;
- АРМ, на которых обрабатывается защищаемая информация;

Далее, были выявлены наиболее существенные угрозы информационной безопасности и разработана модель угроз на основании документа «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка)» ФСТЭК.

Подробное описание модели угроз приведено в пунктах 1.6.1., 1.6.2., 1.6.3.

1.6. Разработка модели угроз и уязвимостей для важных объектов защиты

1.6.1. Угрозы несанкционированного доступа к информации

1.6.1.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн

1.6.1.1.1. Кража ПЭВМ

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн.

В помещении АО «УРАЛПРОМБАНК» введен круглосуточный контроль доступа в контролируемую зону, который осуществляется охранником, двери закрываются на замок, вынос компьютерный техники за пределы помещения возможен только с разрешения охранника.

Вероятность реализации – маловероятна.

1.6.1.1.2. Кража носителей информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями к носителям информации.

В помещении АО «УРАЛПРОМБАНК» введен контроль доступа в контролируемую зону, двери закрываются на замок, ведется учет носителей.

Вероятность реализации – маловероятна.

1.6.1.1.3. Кража ключей и атрибутов доступа

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где происходит работа пользователей.

В помещении АО «УРАЛПРОМБАНК» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.4. Кража, модификация, уничтожение информации

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В помещении АО «УРАЛПРОМБАНК» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.5. Вывод из строя узлов ПЭВМ, каналов связи

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены элементы ИСПДн и проходят каналы связи.

В помещении АО «УРАЛПРОМБАНК» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ

В банке техническое обслуживание ПЭВМ осуществляется сотрудниками, подписавшими соглашение о неразглашении.

Вероятность реализации угрозы – маловероятна.

1.6.1.1.7. Несанкционированное отключение средств защиты

Угроза осуществляется путем НСД внешними и внутренними нарушителями в помещения, где расположены средства защиты ИСПДн.

В помещении АО «УРАЛПРОМБАНК» введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн.

Вероятность реализации угрозы – низкая вероятность.

1.6.1.2. Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных и программных средств.

1.6.1.2.1. Действия вредоносных программ

Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

– скрывать своё присутствие в программной среде компьютера;

– обладать способностью к самокопированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;

– разрушать (искажать произвольным образом) код программ в оперативной памяти;

– выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);

– сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);

– искажать произвольным образом, блокировать и (или) подменять выводимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

Необходимо разработать инструкцию по организации антивирусной защиты.

Вероятность реализации угрозы – низкая вероятность.

1.6.1.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Вероятность реализации угрозы – маловероятна.

1.6.1.2.3. Установка ПО, не связанного с исполнением служебных обязанностей

Угроза осуществляется путем несанкционированной установки ПО внутренними нарушителями, что может привести к нарушению конфиденциальности, целостности и доступности всей ИСПДн или ее элементов.

Все сотрудники проинструктированы о политике установки ПО и осуществляется контроль.

Вероятность реализации угрозы – средняя вероятность.

1.6.1.3. 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

1.6.1.3.1. Утрата ключей и атрибутов доступа

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения парольной политике в части их создания (создают легкие или пустые пароли, не меняют пароли по истечении срока их жизни или компрометации и т.п.) и хранения (записывают пароли на бумажные носители, передают ключи доступа третьим лицам и т.п.) или не осведомлены о них.

В банке отсутствует инструкция по организации парольной защиты.

Вероятность реализации угрозы – высокая вероятность.

1.6.1.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн или не осведомлены о них.

В банке осуществляется резервное копирование обрабатываемых ПДн.

Вероятность реализации угрозы – средняя вероятность.

1.6.1.3.3. Непреднамеренное отключение средств защиты

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения принятых правил работы с ИСПДн и средствами защиты или не осведомлены о них.

В банке введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн. Так же в банке реализовано создание резервных копий, обрабатываемых ПДн.

Вероятность реализации угрозы – средняя вероятность.

1.6.1.3.4. Выход из строя аппаратно-программных средств

Угроза осуществляется вследствие несовершенства аппаратно-программных средств, из-за которых может происходить нарушение целостности и доступности защищаемой информации.

В банке реализовано создание резервных копий, обрабатываемых ПДн.

Вероятность реализации угрозы – средняя вероятность.

1.6.1.3.5. Сбой системы электроснабжения

Угроза осуществляется вследствие несовершенства системы электроснабжения, из-за чего может происходить нарушение целостности и доступности защищаемой информации.

В банке ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – маловероятна.

1.6.1.3.6. Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

В учреждении установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – маловероятна.

1.6.2. Угрозы преднамеренных действий внутренних нарушителей

1.6.2.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке

Угроза осуществляется путем НСД внешних нарушителей в помещения, где расположены элементы ИСПДн и средства защиты, а также происходит работа пользователей.

В помещении АО «УРАЛПРОМБАНК» введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

1.6.2.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке

Угроза осуществляется за счет действия человеческого фактора пользователей ИСПДн, которые нарушают положения о неразглашении обрабатываемой информации или не осведомлены о них.

В учреждении пользователи осведомлены о порядке работы с персональными данными, а также подписали Соглашение о неразглашении.

Требуется установка СЗИ от НСД.

Вероятность реализации угрозы – средняя вероятность.

1.6.3. Угрозы несанкционированного доступа по каналам связи

В соответствии с «Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15 февраля 2008 г.), для ИСПДн можно рассматривать следующие угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

- угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации;
- угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.;
- угрозы выявления паролей по сети;
- угрозы навязывания ложного маршрута сети;
- угрозы подмены доверенного объекта в сети;
- угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях;
- угрозы типа «Отказ в обслуживании»;
- угрозы удаленного запуска приложений;
- угрозы внедрения по сети вредоносных программ.

1.6.3.1. Угроза «Анализ сетевого траффика»

Эта угроза реализуется с помощью специальной программы-анализатора пакетов (sniffer), перехватывающей все пакеты, передаваемые по сегменту сети, и выделяющей среди них те, в которых передаются идентификатор пользователя и его пароль.

Требуется установка СКЗИ.

Вероятность реализации угрозы – средняя вероятность.

1.6.3.2. Угроза «сканирование сети»

Сущность процесса реализации угрозы заключается в передаче запросов сетевым службам хостов ИСПДн и анализе ответов от них. Цель – выявление используемых протоколов, доступных портов сетевых служб, законов формирования идентификаторов соединений, определение активных сетевых сервисов, подбор идентификаторов и паролей пользователей.

В банке установлено антивирусное ПО с сетевыми фильтрами.

Вероятность реализации угрозы – маловероятна.

1.6.3.3. Угроза выявления паролей

Цель реализации угрозы состоит в получении НСД путем преодоления парольной защиты. Злоумышленник может реализовывать угрозу с помощью целого ряда методов, таких как простой перебор, перебор с использованием специальных словарей, установка вредоносной программы для перехвата пароля, подмена доверенного объекта сети (IP-spoofing) и перехват пакетов (sniffing). В основном для реализации угрозы используются специальные программы, которые пытаются получить доступ хосту путем последовательного подбора паролей. В случае успеха, злоумышленник может создать для себя «проход» для будущего доступа, который будет действовать, даже если на хосте изменить пароль доступа.

В учреждении отсутствуют инструкции по организации парольной защиты.

Вероятность реализации угрозы – низкая.

1.6.3.4. Угрозы навязывания ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими алгоритмам маршрутизации (в частности из-за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн.

Требуется установка СКЗИ.

Вероятность реализации угрозы – средняя вероятность.

1.6.3.5. Угрозы подмены доверенного объекта

Такая угроза эффективно реализуется в системах, в которых применяются нестойкие алгоритмы идентификации и аутентификации хостов, пользователей и т.д. Под доверенным объектом понимается объект сети (компьютер, межсетевой экран, маршрутизатор и т.п.), легально подключенный к серверу.

Могут быть выделены две разновидности процесса реализации указанной угрозы: с установлением и без установления виртуального соединения.

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта.

Процесс реализации угрозы без установления виртуального соединения может иметь место в сетях, осуществляющих идентификацию передаваемых сообщений только по сетевому адресу отправителя. Сущность заключается в передаче служебных сообщений от имени сетевых управляющих устройств (например, от имени маршрутизаторов) об изменении маршрутно-адресных данных.

В результате реализации угрозы нарушитель получает права доступа к техническому средству ИСПДн - цели угроз.

Требуется установка СКЗИ.

Вероятность реализации угрозы – средняя.

1.6.3.6. Внедрение ложного объекта сети

Эта угроза основана на использовании недостатков алгоритмов удаленного поиска. В случае если объекты сети изначально не имеют адресной информации друг о друге, используются различные протоколы удаленного поиска, заключающиеся в передаче по сети специальных запросов и получении на них ответов с искомой информацией. При этом существует возможность перехвата нарушителем поискового запроса и выдачи на него ложного ответа, использование которого приведет к требуемому изменению маршрутно-адресных данных. В дальнейшем весь поток информации, ассоциированный с объектом-жертвой, будет проходить через ложный объект сети.

Требуется установка СКЗИ.

Вероятность реализации угрозы – средняя вероятность.

1.6.3.7. Угрозы типа «Отказ в обслуживании»

Эти угрозы основаны на недостатках сетевого программного обеспечения, его уязвимостях, позволяющих нарушителю создавать условия, когда операционная система оказывается не в состоянии обрабатывать поступающие пакеты.

Результатом реализации данной угрозы может стать нарушение работоспособности соответствующей службы предоставления удаленного доступа к ПДн в ИСПДн, передача с одного адреса такого количества запросов на подключение к техническому средству в составе ИСПДн, которое максимально может «вместить» трафик (направленный «шторм запросов»), что влечет за собой переполнение очереди запросов и отказ одной из сетевых служб или полная остановка ИСПДн из-за невозможности системы заниматься ничем другим, кроме обработки запросов.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – маловероятно.

1.6.3.8. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы-закладки, вирусы, «сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль над работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

– распространение файлов, содержащих несанкционированный исполняемый код;

– удаленный запуск приложения путем переполнения буфера приложений-серверов;

– удаленный запуск приложения путем использования возможностей удаленного управления системой, предоставляемых скрытыми программными и аппаратными закладками, либо используемыми штатными средствами.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – маловероятно.

1.6.3.9. Угрозы внедрения по сети вредоносных программ

К вредоносным программам, внедряемым по сети, относятся вирусы, которые для своего распространения активно используют протоколы и возможности локальных и глобальных сетей. Основным принципом работы сетевого вируса является возможность самостоятельно передать свой код на удаленный сервер или рабочую станцию. «Полноценные» сетевые вирусы при этом обладают еще и возможностью запустить на выполнение свой код на удаленном компьютере или, по крайней мере, «подтолкнуть» пользователя к запуску зараженного файла.

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

– программы подбора и вскрытия паролей;

– программы, реализующие угрозы;

– программы, демонстрирующие использование недекларированных возможностей программного и программно-аппаратного обеспечения ИСПДн;

– программы-генераторы компьютерных вирусов;

– программы, демонстрирующие уязвимости средств защиты информации и др.

На всех компьютерах локальной сети установлены антивирусные средства со средствами обнаружения вторжений.

Вероятность реализации угрозы – маловероятно.

1.7. Расчет рисков важных объектов защиты

Расчет рисков важных объектов защиты предприятия АО «УРАЛПРОМБАНК» выполнялся основываясь на документе «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» ФСТЭК.

1.7.1 Вероятность реализации угроз безопасности персональных данных

Под вероятностью реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация

конкретной угрозы безопасности ПДн для ИСПДн в складывающихся условиях обстановки.

Числовой коэффициент (Y2) для оценки вероятности возникновения угрозы определяется по 4 вербальным градациям этого показателя:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

1.7.2. Реализуемость угроз

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y1).

В Таблице 3 представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица 3 – Исходный уровень защищенности

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

ИСПДн имеет средний уровень исходной защищенности, так как не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний».

Показатель исходной защищенности Y1 = 5.

По итогам оценки уровня защищенности (Y1) и вероятности реализации угрозы (Y2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением Y = (Y1 + Y2)/20

Оценка реализуемости угроз безопасности персональных представлена в Таблице 4.

Таблица 4 – Реализуемость угроз

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1	2	3
Угрозы несанкционированного доступа к информации		
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
Кража ПЭВМ	0,25	низкая
Кража носителей информации	0,25	низкая
Кража ключей и атрибутов доступа	0,25	низкая
Кражи, модификации, уничтожения информации	0,25	низкая
Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,25	низкая
Несанкционированное отключение средств защиты	0,25	низкая
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)		
Действия вредоносных программ (вирусов)	0,35	средняя
Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая
Установка ПО не связанного с исполнением служебных обязанностей	0,5	средняя
Угрозы не преднамеренных 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		
Утрата ключей и атрибутов доступа	0,75	высокая
Непреднамеренная модификация (уничтожение) информации сотрудниками	0,35	средняя
Непреднамеренное отключение средств защиты	0,5	средняя

Продолжение таблицы 4

1	2	3
Выход из строя аппаратно-программных средств	0,5	средняя
Сбой системы электроснабжения	0,25	низкая
Стихийное бедствие	0,25	низкая
Угрозы преднамеренных действий внутренних нарушителей		
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	0,25	низкая
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	0,5	средняя
Угрозы несанкционированного доступа по каналам связи		
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации(несерт циско как повлияет)	0,5	средняя
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,25	низкая
Угрозы выявления паролей по сети	0,35	низкая
Угрозы навязывание ложного маршрута сети	0,5	средняя
Угрозы подмены доверенного объекта в сети	0,5	средняя
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,5	средняя
Угрозы типа «Отказ в обслуживании»	0,25	низкая
Угрозы удаленного запуска приложений	0,25	низкая
Угрозы внедрения по сети вредоносных программ	0,25	низкая

1.7.3. Оценка опасности угроз

Оценка опасности УБПДн производится на основе опроса специалистов по защите информации и определяется вербальным показателем опасности, который имеет три значения:

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

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

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

Была произведена оценка опасности УБПДн.

Оценка опасности угроз безопасности персональных данных представлена в Таблице 5.

Таблица 5 – Опасность угроз персональных данных

Тип угроз безопасности ПДн	Опасность угрозы
1	2
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	Низкая
Кража носителей информации	Низкая
Кража ключей и атрибутов доступа	Низкая
Кражи, модификации, уничтожения информации	Низкая
Вывод из строя узлов ПЭВМ, каналов связи	Низкая
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Низкая
Несанкционированное отключение средств защиты	Низкая
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)	
Утрата ключей и атрибутов доступа	Низкая
Непреднамеренная модификация (уничтожение) информации сотрудниками	Низкая
Непреднамеренное отключение средств защиты	Низкая
Выход из строя аппаратно-программных средств	Низкая
Сбой системы электроснабжения	Низкая
Стихийное бедствие	Низкая
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Низкая

Продолжение таблицы 5

1	2
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Низкая
Угрозы выявления паролей по сети	Низкая
Угрозы навязывание ложного маршрута сети	Низкая
Угрозы подмены доверенного объекта в сети	Низкая
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Низкая
Угрозы типа «Отказ в обслуживании»	Низкая
Угрозы удаленного запуска приложений	Низкая
Угрозы внедрения по сети вредоносных программ	Низкая

1.7.4. Определение актуальности угроз

В соответствии с правилами отнесения угрозы безопасности к актуальной, для ИСПДн определяются актуальные и неактуальные угрозы.

Таблица 6 – Определение актуальности угроз

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

Оценка актуальности угроз безопасности представлена в Таблице 7.

Таблица 7 – Актуальность угроз безопасности персональных данных

Тип угроз безопасности ПДн	Актуальность угрозы
1	2
Угрозы несанкционированного доступа к информации	
Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
Кража ПЭВМ	Не актуальная
Кража носителей информации	Не актуальная

Продолжение таблицы 7

1	2
Кража ключей и атрибутов доступа	Не актуальная
Кражи, модификации, уничтожения информации	Не актуальная
Вывод из строя узлов ПЭВМ, каналов связи	Не актуальная
Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	Не актуальная
Несанкционированное отключение средств защиты	Актуальная
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)	
Действия вредоносных программ	Не актуальная
Недекларированные возможности системного ПО и ПО для обработки персональных данных	Не актуальная
Установка ПО не связанного с исполнением служебных обязанностей	Не актуальная
Угрозы не преднамеренных 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	
Утрата ключей и атрибутов доступа	Актуальная
Непреднамеренная модификация (уничтожение) информации сотрудниками	Актуальная
Непреднамеренное отключение средств защиты	Актуальная
Выход из строя аппаратно-программных средств	Не актуальная
Сбой системы электроснабжения	Не актуальная
Стихийное бедствие	Не актуальная
Угрозы преднамеренных действий внутренних нарушителей	
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	Не актуальная
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	Актуальная
Угрозы несанкционированного доступа по каналам связи	
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Актуальная
Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	Не актуальная
Угрозы выявления паролей по сети	Актуальная
Угрозы навязывание ложного маршрута сети	Актуальная
Угрозы подмены доверенного объекта в сети	Актуальная

Продолжение таблицы 7

1	2
Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	Актуальная
Угрозы типа «Отказ в обслуживании»	Не актуальная
Угрозы удаленного запуска приложений	Не актуальная
Угрозы внедрения по сети вредоносных программ	Не актуальная

Таким образом, в отношении персональных данных, обрабатываемых в ИСПДн «КЛИЕНТЫ БАНКА», актуальными являются следующие угрозы безопасности:

– Угрозы НСД:

– несанкционированное отключение средств защиты.

– Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД:

– действия вредоносных программ (вирусов).

– Угрозы не преднамеренных 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:

– утрата ключей и атрибутов доступа;

– непреднамеренная модификация (уничтожение) информации сотрудниками;

– непреднамеренное отключение средств защиты.

– Угрозы преднамеренных действий внутренних нарушителей:

– разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке.

– Угрозы несанкционированного доступа по каналам связи:

– угрозы выявления паролей по сети

– угрозы навязывание ложного маршрута сети

– угрозы подмены доверенного объекта в сети

– угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях

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

1.8. Разработка технического задания на модернизацию системы защиты персональных данных на предприятии АО «УРАЛПРОМБАНК»

По результатам обследования было разработано техническое задание на модернизацию системы защиты персональных данных на предприятии АО «УРАЛПРОМБАНК» (Приложение Б).

В качестве основы был взят ГОСТ 34.602-1989 «Техническое задание на создание автоматизированной системы» [2]. Техническое задание имеет следующие разделы:

1) общие сведения;
2) назначение и цели совершенствования системы;
3) характеристика объектов защиты;
4) требования к ИСПДн;
5) состав и содержание работ по совершенствованию системы;
6) порядок контроля и приемки системы;
7) требования к составу и содержанию работ по подготовке объекта защиты к вводу ИСПДн в действие;
8) требования к документированию;
9) источники разработки.

1.9. Выводы

В результате проведенного обследования СЗИ АО «УРАЛПРОМБАНК», была проделана следующая работа:

– составлен технический паспорт на ИСПДн;
– разработан перечень персональных данных, подлежащих защите в ИСПДн;
– разработана модель угроз безопасности персональных данных и произведена оценка их актуальности;
– разработано техническое задание на модернизацию системы защиты персональных данных на предприятии АО «УРАЛПРОМБАНК».

2.ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1. Обзор возможных методов устранения уязвимостей

Для совершенствования защиты системы информационной обработки персональных данных АО «УРАЛПРОМБАНК», были определены методы и средства, необходимые для устранения выявленных угроз и уязвимостей, определенных в первой главе данной работы, и выбраны из них наиболее эффективные варианты.

2.2. Угрозы несанкционированного доступа к информации

Согласно ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения» [4] 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.

Одним из способов защиты от НСД является использование соответствующих программно-аппаратных средств, которые позволяют управлять доступом к информационной системе, выполнять регистрацию и учет и обеспечивать целостность и неизменность программной среды.

В рамках ВКР был проведен сравнительный анализ программно-аппаратных средств защиты от НСД, результаты которого приведены в Таблице 8.

Таблица 8 – Сравнение СЗИ от НСД

Критерии сравнения	Secret Net Studio	Dallas Lock 8.0-K	СЗИ Аура 1.2.4.
1	2	3	4
Сертификат	ФСТЭК № 3745 действителен до 16.05.2020	ФСТЭК № 2720 действителен до 25.09.2018	ФСТЭК № 2527 действителен до 26.12.2020
Класс защищенности	По 5 классу защищенности	По 5 классу защищенности	По 5 классу защищенности
Уровень контроля НДВ	По 4 уровню контроля	По 4 уровню контроля	По 4 уровню контроля
Уровень защищенности ИСПДн	До 1 уровня включительно	До 1 уровня включительно	До 1 уровня включительно
Дополнительная аппаратая поддержка	есть	есть	нет
Цена	8175	8500	5000

На основании разработанной модели угроз угрозы связанные с НСД были признаны актуальными. Для их минимизации были выбраны ПАК «Dallas Lock 8.0-K» из-за выгодного соотношения цена/функциональность. Так же была разработана инструкция по организации антивирусной защиты.

2.3. Угрозы преднамеренных действий внутренних нарушителей

Данные угрозы являются наиболее распространенными и, соответственно, наиболее важными с точки зрения защиты информации, так как больший приоритет имеет защита информации ограниченного доступа от преднамеренных действий внутренних нарушителей, а именно сотрудников, допущенных к ее обработке.

Для АО «УРАЛПРОМБАНК» актуален данный вид угроз и рекомендуются следующие меры для их минимизации:

- установка СЗИ от НСД «Dallas Lock 8.0-K»;
- разработка инструкции по организации антивирусной защиты.

2.4. Угрозы несанкционированного доступа по каналам связи

Данный вид угроз заключается в передаче запросов сетевым узлам и анализе ответов на них, в результате чего может быть получена топология сети, выявлены открытые уязвимые порты, используемые протоколы, активные сетевые сервисы.

В ходе анализа результатов обследования было установлено, что, для АО «УРАЛПРОМБАНК» актуальны 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.

Для защиты от этих угроз необходимо применение межсетевых экранов. В ИСПДн установлен Межсетевой экран Cisco ASA 5510.

Так же разработана инструкция по организации парольной защиты.

2.5. Выводы

На основе результатов работ по выявлению уязвимостей на рассматриваемом предприятии, приводящих к реализации возможных угроз, были применены следующие меры по их минимизации:

1. Для защиты от угроз несанкционированного доступа к информации:
   - установлены СЗИ от НСД «Dallas Lock 8.0-K» по причине наилучшего соотношения цена/функциональность из сравниваемых СЗИ от НСД в Таблице 9.
2. Для защиты от угроз преднамеренных действий внутренних нарушителей:
   - установлены СЗИ от НСД «Dallas Lock 8.0-K;
   - разработана инструкция по организации антивирусной защиты.

3. РАЗРАБОТКА ТЕХНИЧЕСКОГО ЗАДАНИЯ МОДЕРНИЗАЦИИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ НА ПРЕДПРИЯТИИ АО «УРАЛПРОМБАНК»

3.1. Описание объекта

АО «УРАЛПРОМБАНК» — небольшой по размеру активов региональный банк. Основные направления деятельности — обслуживание и кредитование предприятий и организаций Челябинской области, операции на долговом и межбанковском рынках.

3.2. Резюме технического задания

Модернизация системы защиты должно осуществляться с помощью организационных, инженерно-технических и программно-аппаратных мер. На каждый конкретный этап работ должны быть назначены ответственные лица с помощью матрицы ответственности.

Результатом работ должна стать обновлённая система защиты персональных данных АО «УРАЛПРОМБАНК», соответствующая нормативно-правовым актам в области защиты персональных данных.

3.3. Цели и задачи технического задания

Целями модернизации системы защиты персональных данных АО «УРАЛПРОМБАНК» являются:

– предотвращение угроз, связанных с НСД;

– предотвращение угроз преднамеренных действий внутренних нарушителей;

– предотвращение угроз несанкционированного доступа по каналам связи;

– защита нового рабочего места;

– осуществление защиты персональных данных в соответствии с нормативно-правовыми актами.

3.4. Объекты поставки технического задания

3.4.1. Организационно-распорядительная документация

Организационно-распорядительная документация на предприятии АО «УРАЛПРОМБАНК»:

– инструкция по организации антивирусной защите (Приложение Г);

– инструкция по парольной защите(Приложение Е);

– перечень персональных данных, подлежащих защите в информационной системе обработки персональных данных (Приложение В);

– технический паспорт на информационную систему обработки персональных данных (Приложение А);

– акт классификации ИСПДн (Приложение Д);

– техническое задание на модернизацию системы защиты персональных данных (Приложение Б);

– письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных(Приложение Ж).

3.4.2. Программно-аппаратные и инженерно-технические меры

В рамках реализации технического задания по модернизации системы защиты персональных данных были закуплены и установлены следующие программно-аппаратные средства:

– на старые АРМ: СЗИ от НСД «Dallas Lock 8.0-K»;

– на новое АРМ: Антивирусное ПО «Kaspersky Endpoint Security 10 для Windows», СЗИ от НСД «Dallas Lock 8.0-K».

3.5. Структура разбиения работ

ИСПДн 1. Проектирование;

ИСПДн 1.1. Определение ключевых показателей существующих бизнес-процессов с точки зрения ИБ;

ИСПДн 1.2. Анализ проблем и слабых мест существующих бизнес процессов;

ИСПДн 1.3. Разработка значений ключевых показателей новых бизнес-процессов;

ИСПДн 1.4. Анализ и выбор наилучших способов и методов улучшения значений ключевых показателей бизнес-процессов;

ИСПДн 1.5. Разработка и согласование структуры новых бизнес-процессов.

ИСПДн 2. Совершенствование организационно-распорядительной документации;

ИСПДн 2.1. Технический паспорт;

ИСПДн 2.2. Инструкция по организации антивирусной защиты;

ИСПДн 2.3. Инструкция по организации парольной защиты;

ИСПДн 2.4. Согласование и утверждение ОРД.

ИСПДн 3. Подготовка реализации технического модернизации системы защиты персональных данных;

ИСПДн 3.1. Определение ответственных лиц и исполнителей технического задания;

ИСПДн 3.2. Приобретение СЗИ от НСД;

ИСПДн 3.3. Приобретение антивирусного ПО.

ИСПДн 4. Внедрение;

ИСПДн 4.1. Установка и настройка СЗИ от НСД;

ИСПДн 4.2. Установка и настройка антивирусного ПО;

ИСПДн 4.3. Контроль защищенности.

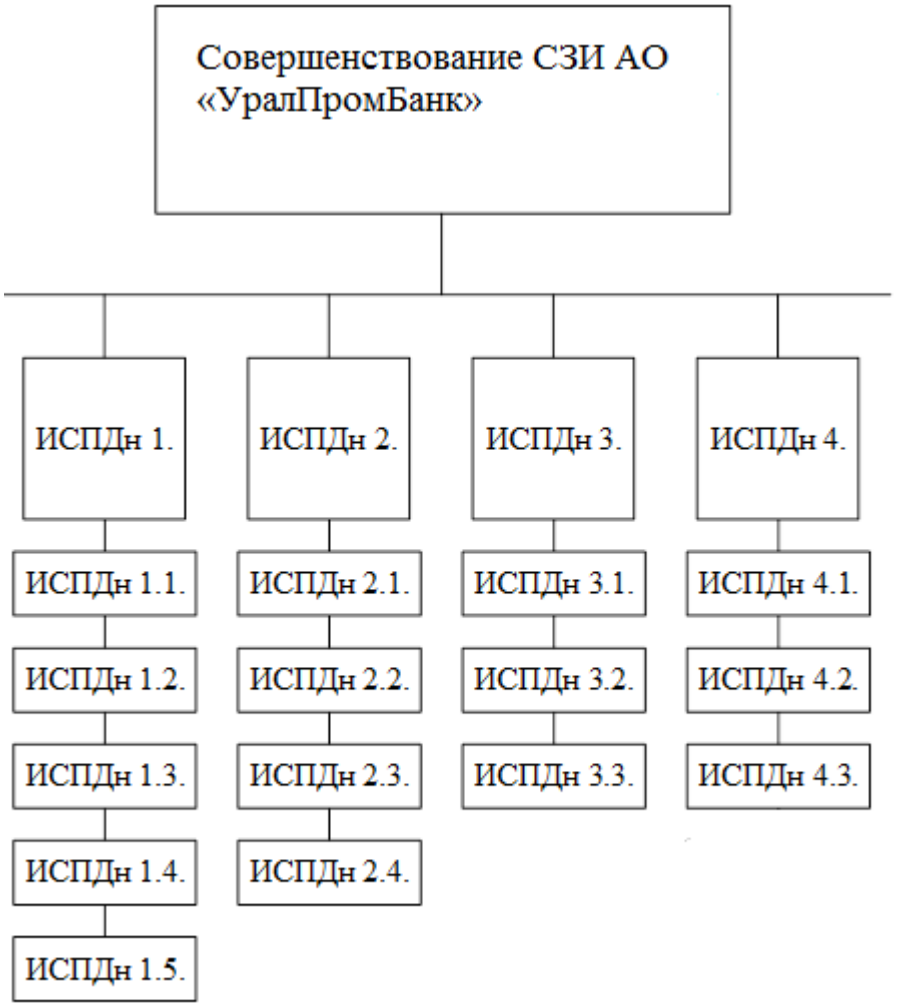

Рисунок 1 – Структура разбиения работ

3.6. Структурная схема организации технического задания

Структурная схема организации технического задания модернизации системы защиты персональных данных приведена на Рисунке 2.

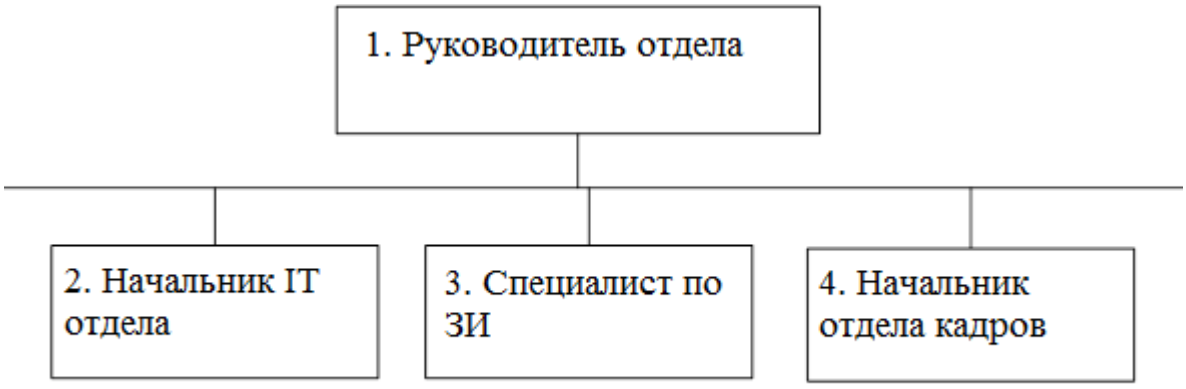

Рисунок 2 – Структурная схема организации технического задания

3.7. Матрица ответственности

Для наглядности обязанностей исполнителей технического задания составляется матрица ответственности (Таблица 9). Работа исполнителей разделяется на следующие группы: управление (У), исполнение (И), контроль (К).

Таблица 9 – Матрица ответственности

Исполнитель/Работа	1	2	3	4
ИСПДн 1.	К/У			
ИСПДн 1.1.	К		И	
ИСПДн 1.2.	К		И/К	
ИСПДн 1.3	К		И/К	
ИСПДн 1.4.	К		И	
ИСПДн 1.5.	К		И/К	
ИСПДн 2.	К		У/И	
ИСПДн 2.1.	К		У/И	
ИСПДн 2.2.	К		У/И	
ИСПДн 2.3.	К		У/И	
ИСПДн 2.4.	К		У/И	
ИСПДн 3.	К			
ИСПДн 3.1.	К			
ИСПДн 3.2.	К			
ИСПДн 3.3.	К			
ИСПДн 4.	К			
ИСПДн 4.1.	К	И		
ИСПДн 4.2.	К	И		
ИСПДн 4.3.	К			И

3.8. Выводы

В результате выполненных работ по реализации технического задания по модернизации системы защиты персональных данных АО «УРАЛПРОМБАНК» было сделано:

– подготовлен комплект организационно-распорядительной документации;

– закуплены и установлены программно-аппаратные средства защиты информации;

– проведён инструктаж сотрудников по антивирусной и парольной защите;

– было проведено разбиение работ и на его основе составлена матрица ответственности.

4. РАСЧЁТ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ

4.1. Перечень средств защиты информации.

Для модернизации защиты ИСПДн необходимо произвести закупку СЗИ. Для помещения АО «УРАЛПРОМБАНК» необходимо установить СЗИ Dallas Lock 8.0-K, Kaspersky Endpoint Security 10.

Стоимость СЗИ отражена в таблице 10.

Таблица 10 – Стоимость СЗИ

Наименование	Количество	Стоимость (за шт.)	Итоговая стоимость
Dallas Lock 8.0-K	5	7500	37500
Kaspersky Endpoint Security 10	1	2400	2400
Итого			39900

Первоначальные затраты включают в себя закупку СЗИ, и составляют 39900 р. Постоянной затратой будет продление лицензии на использование СЗИ Kaspersky Endpoint Security 10, у остальных СЗИ лицензия действует без продления. Выгодой является отсутствие необходимости в разработке документации на ИСПДн, поскольку она была оформлена в рамках выпускной квалификационной работы. Так же в качестве выгоды посчитана максимальная сумма штрафа, согласно Статье 13.11 КоАП «Нарушение законодательства Российской Федерации в области персональных данных».

4.2. Определение чистой стоимости реализации ТЗ

Чтобы определить, будет успешным техническое задание финансовыми специалистами используется определенный метод оценки – NPV.

Таблица 11 - Чистая приведенная стоимость реализации ТЗ (руб.)

Периоды	0	1	2	3	4
Первоначальные инвестиции	- 37500				
Постоянные инвестиции (продление антивирусного ПО)			- 2400	- 2400	- 2400
Выгоды		291 000	291 000	291 000	291 000
Итого	- 37500	291 000	288 600	288 600	288 600

NPV — это сокращение по первым буквам фразы «NetPresentValue» и расшифровывается это как чистая приведенная (к сегодняшнему дню) стоимость. Это метод оценки, основанный на методологии дисконтирования денежных потоков. Рассчитывается NPV по Формуле (1):

$$NPV = \sum_{t=0}^{n} \frac{CF_t}{(1+R)^t}, \quad (1)$$

где CF – денежный поток;
R – стоимость капитала (ставка дисконтирования);
n, t – количество временных периодов.

Ставку дисконтирования примем эквивалентной ключевой ставке центрального банка – 9,25 %.

$$NPV = \frac{CF^0}{(1+R)^0} + \frac{CF^1}{(1+R)^1} + \frac{CF^2}{(1+R)^2} + \frac{CF^3}{(1+R)^3} =$$

$$= \frac{(-37500 + 291000)}{(1+0{,}0925)^0} + \frac{288600}{(1+0{,}0925)^1} + \frac{288600}{(1+0{,}0925)^2} + \frac{288600}{(1+0{,}0925)^3} =$$

$$= 234290 + 248780 + 227715 + 208435 = 919\,210 \textit{ руб.}$$

Так как NPV больше нуля, значит данное техническое задание на модернизацию системы защиты персональных «КЛИЕНТЫ БАНКА» на предприятии АО «УРАЛПРОМБАНК» экономически эффективно.

4.3. Выводы

Был проведён расчёт бюджета технического задания.

Экономическая эффективность была обоснована, при помощи нахождения чистой приведённой стоимости технического задания.

5. БЕЗОПАСНОСТЬ ЖИЗНЕДЕЯТЕЛЬНОСТИ

5.1. Введение

Объектом выпускной квалификационной работы является дополнительный офис №5 АО «УРАЛПРОМБАНК» г. Коркино. Целью работы является модернизация защиты ИСПДн. Обработка ПДн ведется с помощью персональных электронно-вычислительных машин (далее – ПЭВМ). При работе с ПЭВМ работник подвергается действию шума, так же возможна опасность возникновения возгорания или поражения электрическим током. Так же на здоровье влияет освещение и микроклимат в помещении.

5.1. Рекомендации по организации рабочего места пользователя

Рассмотрим СанПиН 2.2.2/2.4.1340-03, где предъявляются основные требования к рабочему месту сотрудников:

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

Конструкция рабочего стула (кресла) должна обеспечивать поддержание рациональной рабочей позы при работе на ПК, позволять 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 ПК.

Рабочий стул (кресло) должен быть обеспечен подъемно-поворотным механизмом, также он должен 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.

По отношению к световым проемам, ПК должны располагаться так, чтобы естественный свет падал сбоку, преимущественно слева. Свет, падающий спереди на рабочее место, утомляет зрение. Свет, падающий сзади, ухудшает видимость, создает блики на экране.

Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680 - 800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм. Рабочее место пользователя ПК следует оборудовать подставкой для ног. 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.

5.2. Рекомендации по выбору помещения для рабочего места

При работе с вычислительной техникой важным фактором, обеспечивающим высокий уровень работоспособности, является правильно спроектированное помещение, в котором будут располагаться рабочие места, оборудование ЭВМ с ВДТ.

По требованиям СанПиН 2.2.2/2.4.1340-03 «Гигиенические требования к персональным электронно-вычислительным машинам и организации работы» 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 м2 и 6 м2 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.

5.3. 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 12). Параметры требований к микроклимату для работ различных категорий приведены в СанПиН 2.2.4.3359-16 [9].

Таблица 12 – 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
1	2	3	4	5	6
Холодный	Iа (до 139)	22 – 24	21 – 25	60 – 40	0,1

Продолжение таблицы 12

1	2	3	4	5	6
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.

5.4. 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. А именно должен соответствовать нормам СанПиН 2.2.4.3359-16 для высококвалифицированной работы, требующей сосредоточенности, в рабочих комнатах.

В соответствии с нормами, ограничивающими 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.

5.5 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.

5.6 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 видеомонитора и экрана другого видеомонитора), должно быть не менее 2,0 м, а расстояние между боковыми поверхностями видеомониторов – 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 видеомонитора 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 [10], 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.

5.7 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» [11].

5.8 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.

На основе ФЗ «Технический регламент о требованиях пожарной безопасности» 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 ра-

бот 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 каждого 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).

5.9 Рекомендации по организации режима труда и отдыха

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.

5.10 Сравнение параметров рабочего места с допустимыми нормами.

Для определения соответствия условий труда требованиям нормативных документов проведем сравнительный анализ требований, установленных к рабочим местам, оборудованным ПЭВМ и фактических параметров рабочего места. Схема размещения рабочего места приведена на Рисунке 1. Площадь помещения 28м^2, оконный проем, шириной 2,5м размещается по центру. В помещении используют регулируемые стулья и подставки для ног. В помещении присутствует естественное и искусственное освещение. Окно выходит на юг. Естественный свет падает сбоку (слева).

Перечень нормируемых параметров для рабочего места, сравнение их допустимых нормы и фактические значений на рабочем месте представлены в таблице 13.

Рис. 3 – Схема рабочего места.

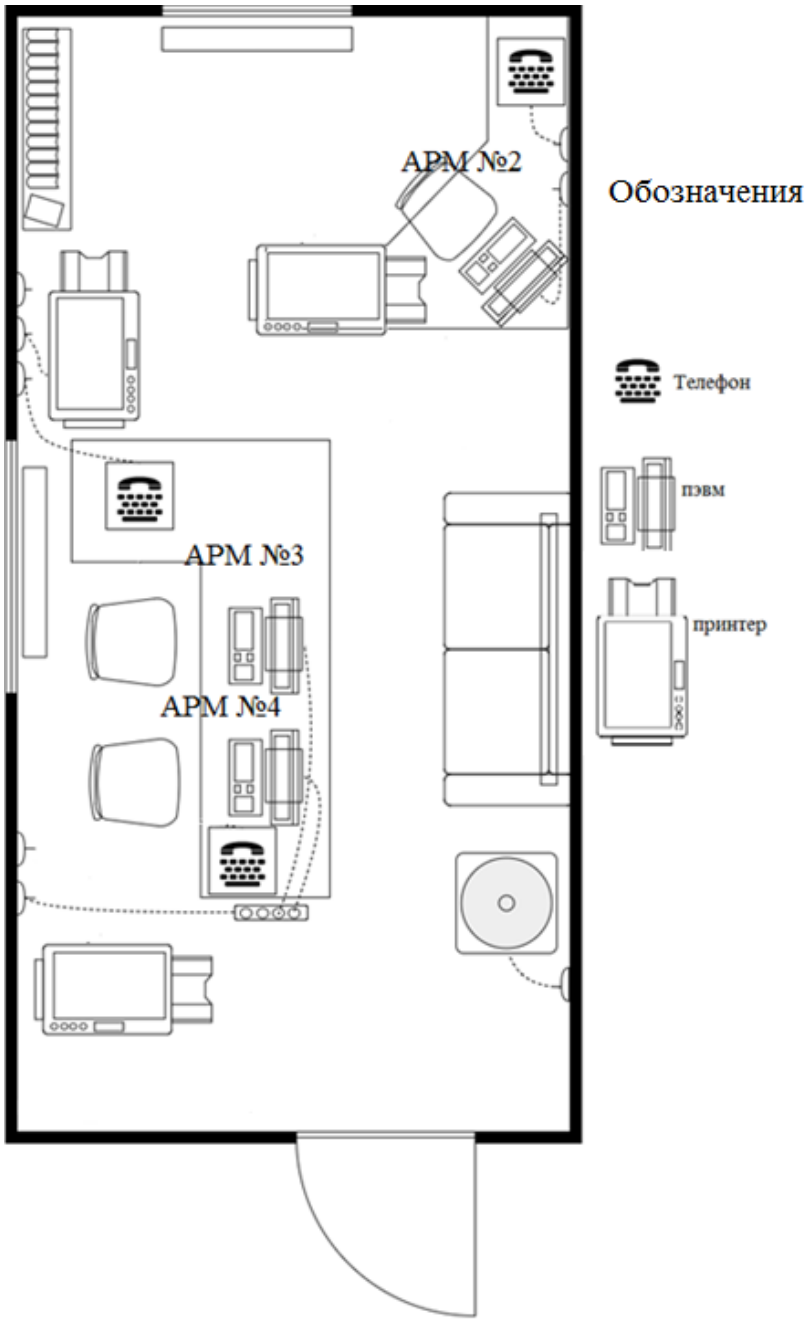

Таблица 13 – Сравнение параметров рабочего места с допустимыми нормами.

Нормируемые параметры	Допустимые нормы	Фактические значения
1	2	3
Высота рабочей поверхности стола	от 680 до 800мм, либо 725мм	700мм
Модульные размеры рабочей поверхности стола	Ширина 800, 1000, 1200, 1400мм, глубина 800 и 1000мм	Ширина 1200мм глубина 1000

Продолжение таблицы 13

1	2	3
Ширина и глубина поверхности сиденья	Не менее 400мм	Ширина 600мм Глубина 450мм
Площадь на одно рабочее место	не менее 4,5м2	10м2
Падение естественного света	Преимущественно слева	Слева
Освещенность поверхности стола	300-500 лк	452 лк
Уровень звука	80 дБА	40 дБА
Параметры микроклимата (кат. 1а)	Температура воздуха 22-24° С Влажность воздуха 40-60%	Температура 23° С Влажность воздуха 43%

5.11. Вывод

В данной главе были установлены требования и рекомендации к работе в организации. Были установлены требования к помещениям, в которых располагаются рабочие места. Установлены требования к уровням шума и микроклимату на рабочих местах.

Выявлены основные требования к освещению на рабочих местах. Так же указаны общие требования к организации рабочих мест пользователей. Указаны требования к электробезопасности. Даны рекомендации по организации режима труда и отдыха пользователя.

На основе проведенного анализа было установлено, что условия труда на рабочем месте соответствуют вышеперечисленным требованиям.

ЗАКЛЮЧЕНИЕ

В результате проведения выпускной квалификационной работы был проведен анализ состояния защиты информации на предприятии АО «УРАЛПРОМБАНК». В ходе обследования были выявлены уязвимости в существующей системе защиты информации и отсутствие части организационно-распорядительной документации в области защиты информации. По этой причине были разработаны необходимые организационно-распорядительные документы и установлены программно-аппаратные средства защиты информации.

Результатами выпускной квалификационной работы стали:

– Разработан технический паспорт на информационную систему – был проведен осмотр помещений и технических средств, составлены их перечни и схемы расположения;

– Разработана модель угроз и уязвимостей для информационной системы на основе базовой модели угроз безопасности ФСТЭК;

– Разработано техническое задание на модернизацию системы защиты информации на предприятии АО «УРАЛПРОМБАНК»;

– Проведена оценка экономической эффективности технического задания, по ее результатам внедрение системы защиты экономически целесообразно.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. «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.
2. ГОСТ 34.602-1989. Техническое задание на создание автоматизированной системы. – М.: Изд-во стандартов, 1990. – 12 с.
3. ГОСТ Р 12.1.019-2009. Система стандартов безопасности труда. Электробезопасность. Общие требования и номенклатура видов защиты. – М.: Изд-во стандартов, 2010. – 32 с.
4. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. – Введ. 2008–02–01. – М.: Госстандарт России, 2001. – 12 с.
5. 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.
6. «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.
7. Постановление правительства РФ «Об утверждении требований к защите 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.
8. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»: утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30.03.1992 // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2016.
9. СанПин 2.2.2/2.4.1340-03. Гигиенические требования к персональным электронно-вычислительным машинам и огранизации работы. – М.: Изд-во стандартов, 2003. – 36 с.
10. 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.
11. СанПин 2.2.4.3359-16. Санитарно-эпидемологические требования к физическим факторам на рабочих местах. – М.: Изд-во стандартов, 2016. – 72 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. 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.

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

17. Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (СТО БР ИББС-1.0-2014)

ПРИЛОЖЕНИЕ А

УТВЕРЖДАЮ
Руководитель дополнительного офиса №5 АО «УРАЛПРОМБАНК»
_____
«____» _____ 2018 г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
на объект информатизации
ИСПДн«КЛИЕНТЫ БАНКА»
Акционерного общества «УРАЛПРОМБАНК»

СОСТАВИЛ

_____ В.Д. Лопатин

«____» _____ 2018 г.

2018 г.

1 ОБЩИЕ СВЕДЕНИЯ ОБ ОБЪЕКТЕ

1.1 Наименование объекта: ИСПДн «КЛИЕНТЫ БАНКА» акционерного общества «УРАЛПРОМБАНК».

1.2 Расположение объекта: Челябинская обл., г. Коркино, ул. Мира, д. 35.

1.3 Классификация объекта: уровень защищённости ИСПДн – 3, «Акт защищённости…» 2018 г.

2 СОСТАВ ОБОРУДОВАНИЯ ОБЪЕКТА

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

Таблица 2.1 – Перечень ОТСС, входящих в состав ОИ ИСПДн «КЛИЕНТЫ БАНКА»

Наименование устройства	**Фирма производитель, модель**	**Заводской / инвентаризационный номер**	**Расположение**
1	2	3	4
Межсетевой экран	Cisco 5510		Рисунок 2.1
АРМ №1			
Системный блок	HP260	a102urZ0J78EA	Рисунок 2.1
Твердотельный накопитель	WD WD3200AAKX-001CA0	WD-WCAYUAA20921	Рисунок 2.1
Монитор	LG L1942S-BF	907NDBP3G709	Рисунок 2.1
Клавиатура	Genius K639	ZM7902171374	Рисунок 2.1
Мышь	OKLICK 225M	0907	Рисунок 2.1
ИБП	APC SmartuPS 500	QS0614121487	Рисунок 2.1
Принтер	HP LaserJet 1018	CNC1L86960	Рисунок 2.1
АРМ №2			
Системный блок	HP260	a102urZ0J78EA	Рисунок 2.1
Твердотельный накопитель	WD WD3200AAKX-001CA0	WD-WCAYUAA20921	Рисунок 2.1
Монитор	LG L1942S-BF	907NDBP3G709	Рисунок 2.1
Клавиатура	Genius K639	ZM7902171374	Рисунок 2.1
Мышь	OKLICK 225M	0907	Рисунок 2.1
ИБП	APC SmartuPS 500	QS0614121487	Рисунок 2.1
Принтер	HP LaserJet 1018	CNC1L86960	Рисунок 2.1
Камера	Rekam A140	RE17137421	Рисунок 2.1
АРМ №3			
Системный блок	HP260	a102urZ0J78EA	Рисунок 2.1

Твердотельный накопитель	WD WD3200AAKX-001CA0	WD-WCAYUAA20921	Рисунок 2.1
Монитор	LG L1942S-BF	907NDBP3G709	Рисунок 2.1
Клавиатура	Genius K639	ZM7902171374	Рисунок 2.1
Мышь	OKLICK 225M	0907	Рисунок 2.1
ИБП	APC SmartuPS 500	QS0614121487	Рисунок 2.1
Принтер	HP LaserJet 1018	CNC1L86960	Рисунок 2.1
Камера	Rekam A140	RE17137421	Рисунок 2.1
АРМ №4			
Системный блок	HP260	a102urZ0J78EA	Рисунок 2.1
Твердотельный накопитель	WD WD3200AAKX-001CA0	WD-WCAYUAA20921	Рисунок 2.1
Монитор	LG L1942S-BF	907NDBP3G709	Рисунок 2.1
Клавиатура	Genius K639	ZM7902171374	Рисунок 2.1
Мышь	OKLICK 225M	0907	Рисунок 2.1
ИБП	APC SmartuPS 500	QS0614121487	Рисунок 2.1
Принтер	HP LaserJet 1018	CNC1L86960	Рисунок 2.1
Камера	Rekam A140	RE17137421	Рисунок 2.1
АРМ №5			
Системный блок	HP260	a102urZ0J78EA	Рисунок 2.1
Твердотельный накопитель	WD WD3200AAKX-001CA0	WD-WCAYUAA20921	Рисунок 2.1
Монитор	LG L1942S-BF	907NDBP3G709	Рисунок 2.1
Клавиатура	Genius K639	ZM7902171374	Рисунок 2.1
Мышь	OKLICK 225M	0907	Рисунок 2.1
ИБП	APC SmartuPS 500	QS0614121487	Рисунок 2.1
Принтер	HP LaserJet 1018	CNC1L86960	Рисунок 2.1
МФУ	HP LaserJet Pro	CNC1L251230	Рисунок 2.1

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

Таблица 2.2 – Перечень ВТСС ОИ ИСПДн «КЛИЕНТЫ БАНКА»

Наименование устройства	**Фирма производитель, модель**	**Заводской / инвентаризационный номер**	**Расположение**	**Количество**
Камера	Falcon Eye	FE-B720AHD	Рисунок 2.2	3
Пульт ОПС	б/н		Рисунок 2.2	1
Телефонный аппарат	Panasonic KX	TS2352	Рисунок 2.2	5
Датчик пожарной сигнализации	б/н		Рисунок 2.2	5
АРМ №6				
Системный блок	HP260	a102urZ0J78EA	Рисунок 2.2	1
Твердотельный накопитель	WD WD3200AAKX -001CA0	WD-WCAYUAA20921	Рисунок 2.2	1
Монитор	LG L1942S-BF	907NDBP3G709	Рисунок 2.2	1
Клавиатура	Genius K639	ZM7902171374	Рисунок 2.2	1
Мышь	OKLICK 225M	0907	Рисунок 2.2	1
ИБП	APC SmartuPS 500	QS0614121487	Рисунок 2.2	1
Телефонный аппарат	Panasonic KX	TS2352	Рисунок 2.2	1

2.3 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.

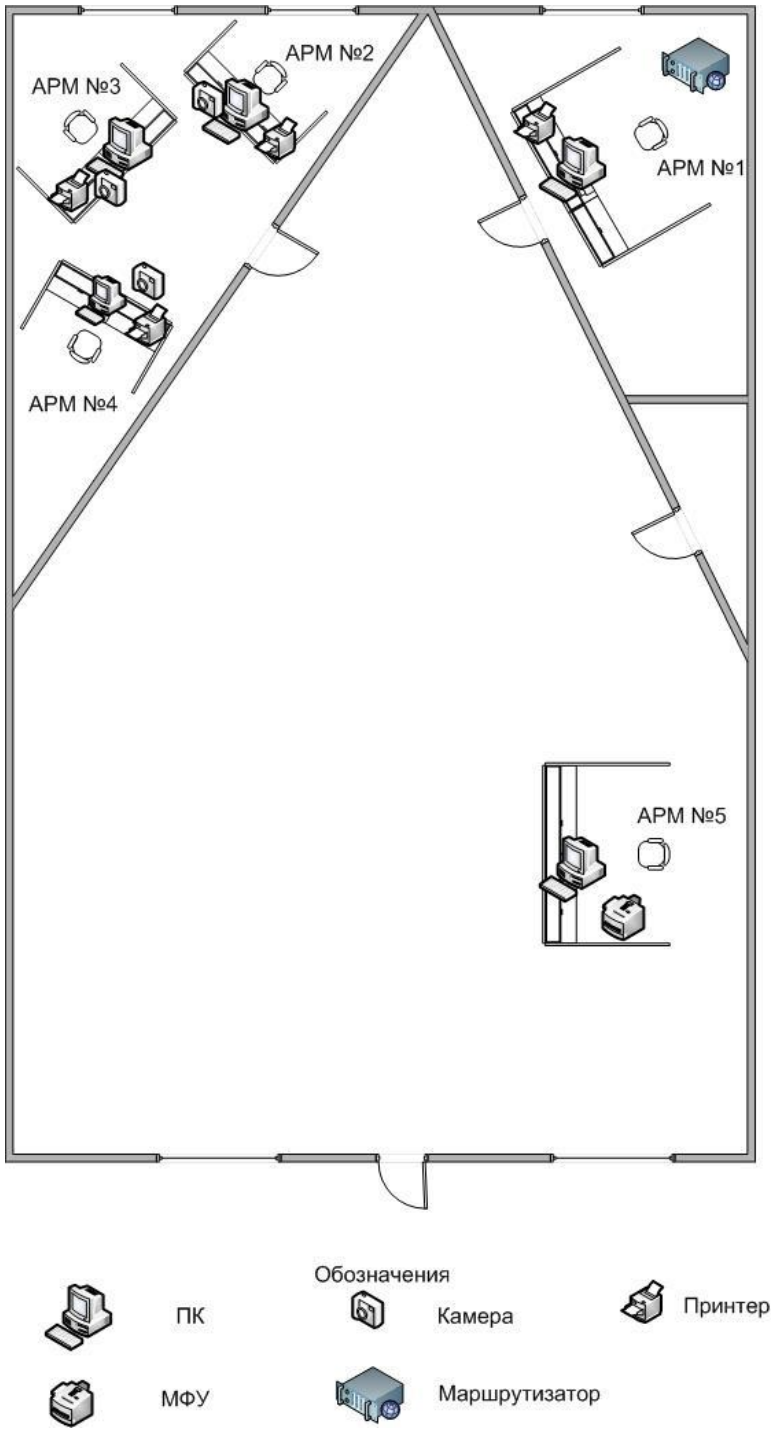

Рисунок 2.1 – Размещение ОТСС ИСПДн «КЛИЕНТЫ БАНКА»
*Примечание: Обозначения 1-10 приведены в Таблице 2.1 основной части технического паспорта.

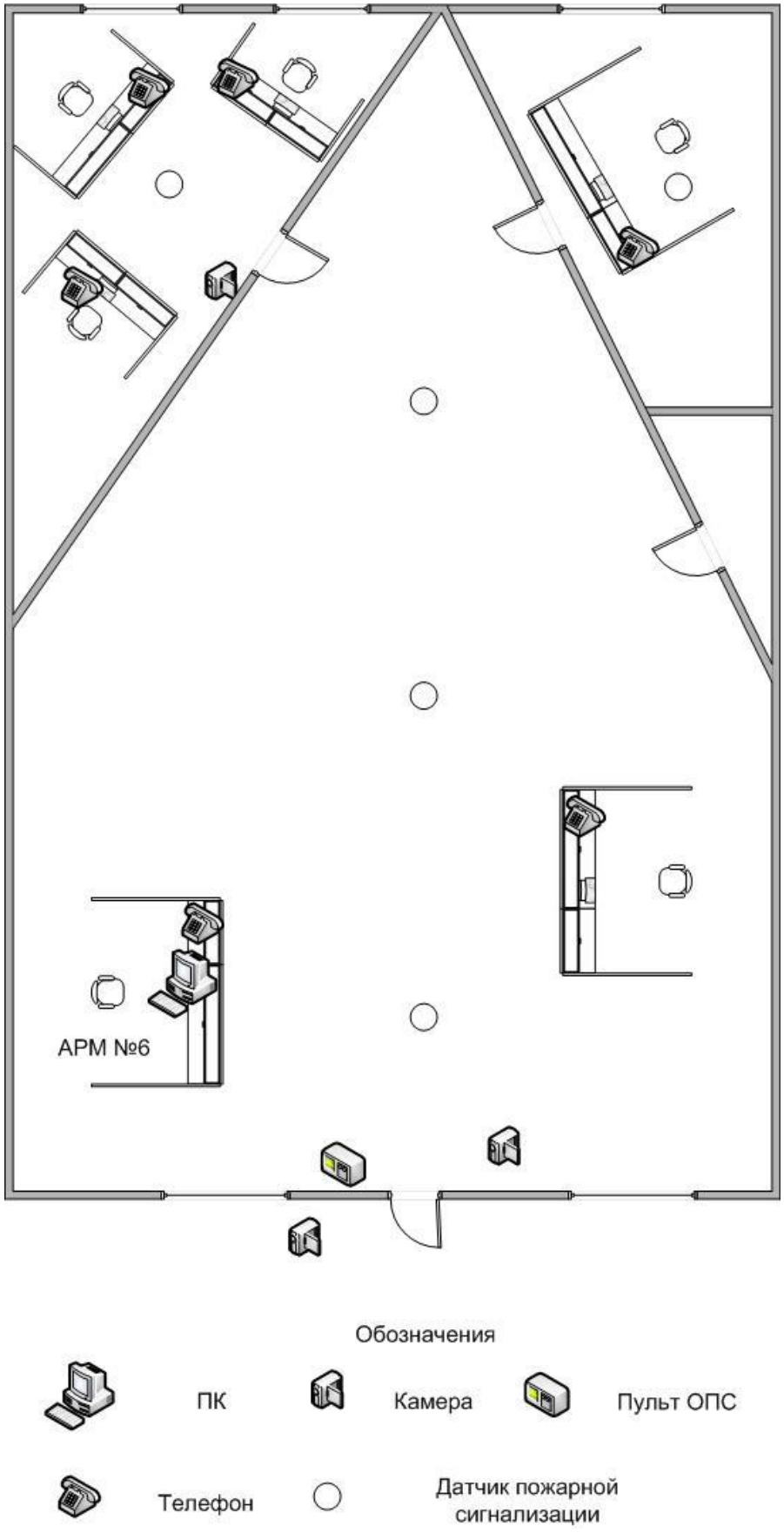

Рисунок 2.2 – Размещение ВТСС ИСПДн «КЛИЕНТЫ БАНКА»

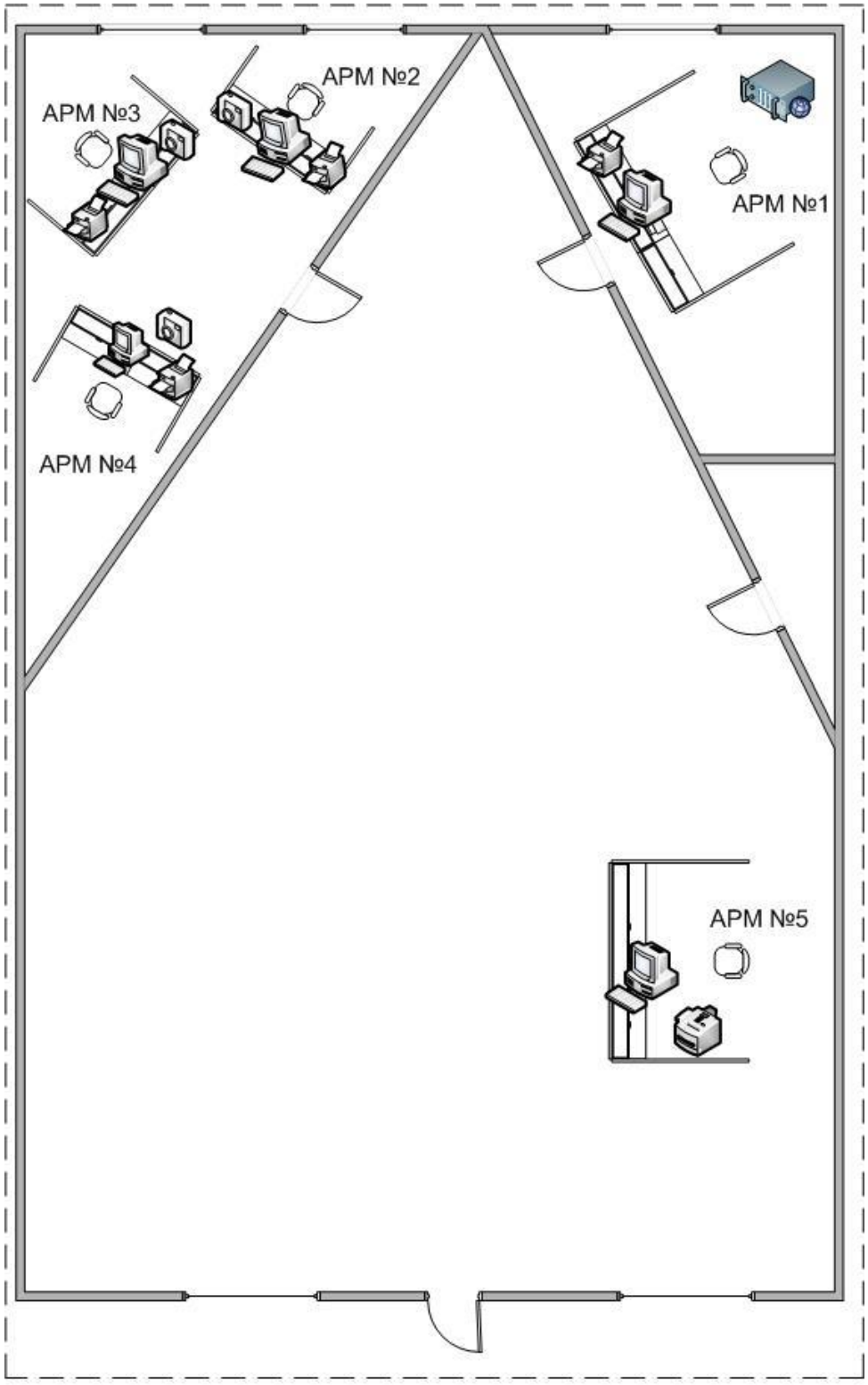

Рисунок 2.3 – Размещение ОТСС относительно границ контролируемой зоны

Границей контролируемой зоной являются стены помещения Акционерного общества «УРАЛПРОМБАНК» Челябинская обл., г. Коркино, ул. Мира, д. 35, согласно приказу «Об определении границ контролируемой зоны объекта информатизации ИСПДн«КЛИЕНТЫ БАНКА» № 77 от 11.02.2016 г.

Объект располагается на первом этаже. Минимальное расстояние от ОТСС до КЗ составляет 1 метр.

2.4 Размещение линий телефонной связи показано на рисунке 2.4.

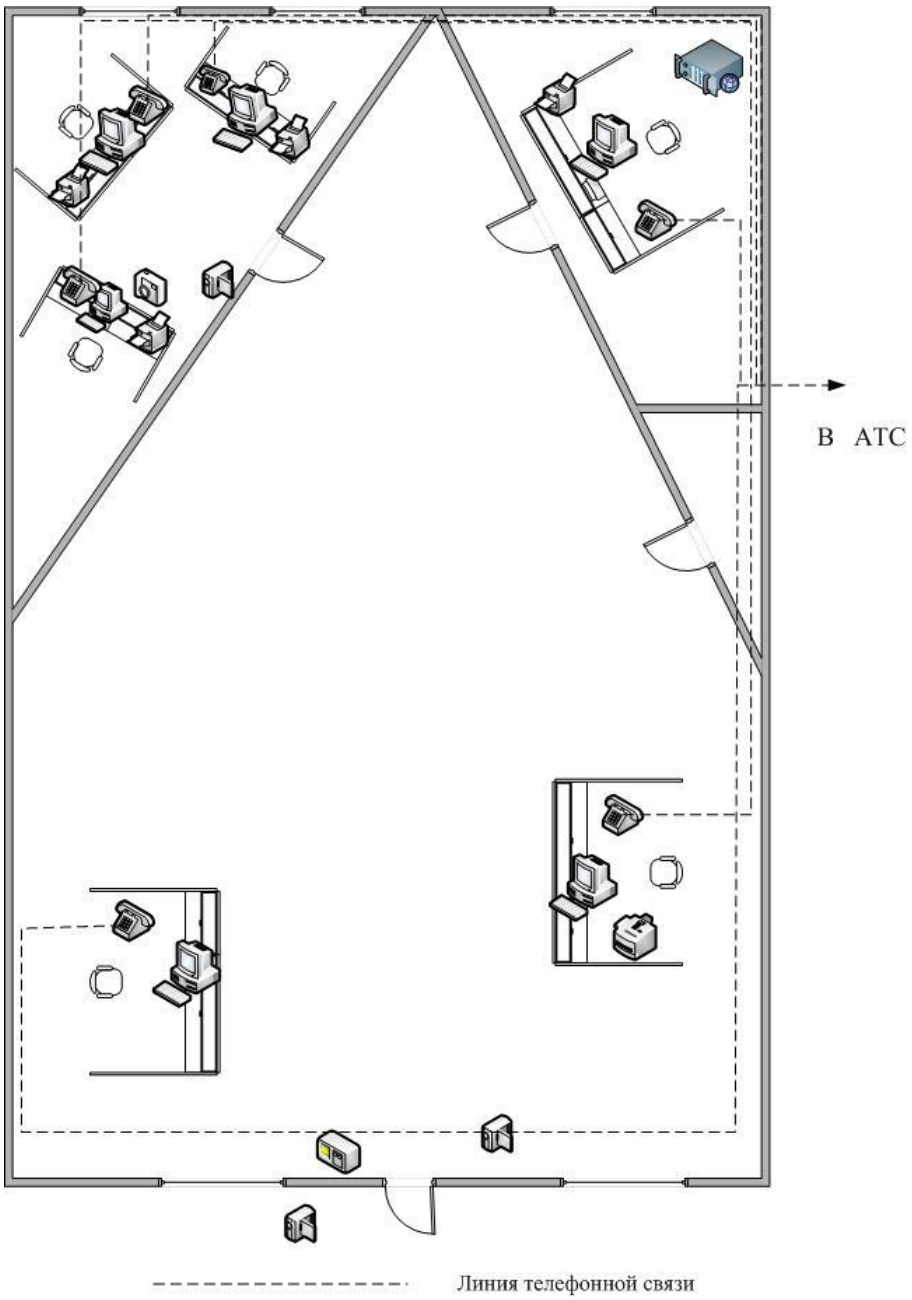

Рисунок 2.4 – Размещение линий телефонной связи

2.5 Размещений линий локально-вычислительной сети приведено на рисунке 2.5.

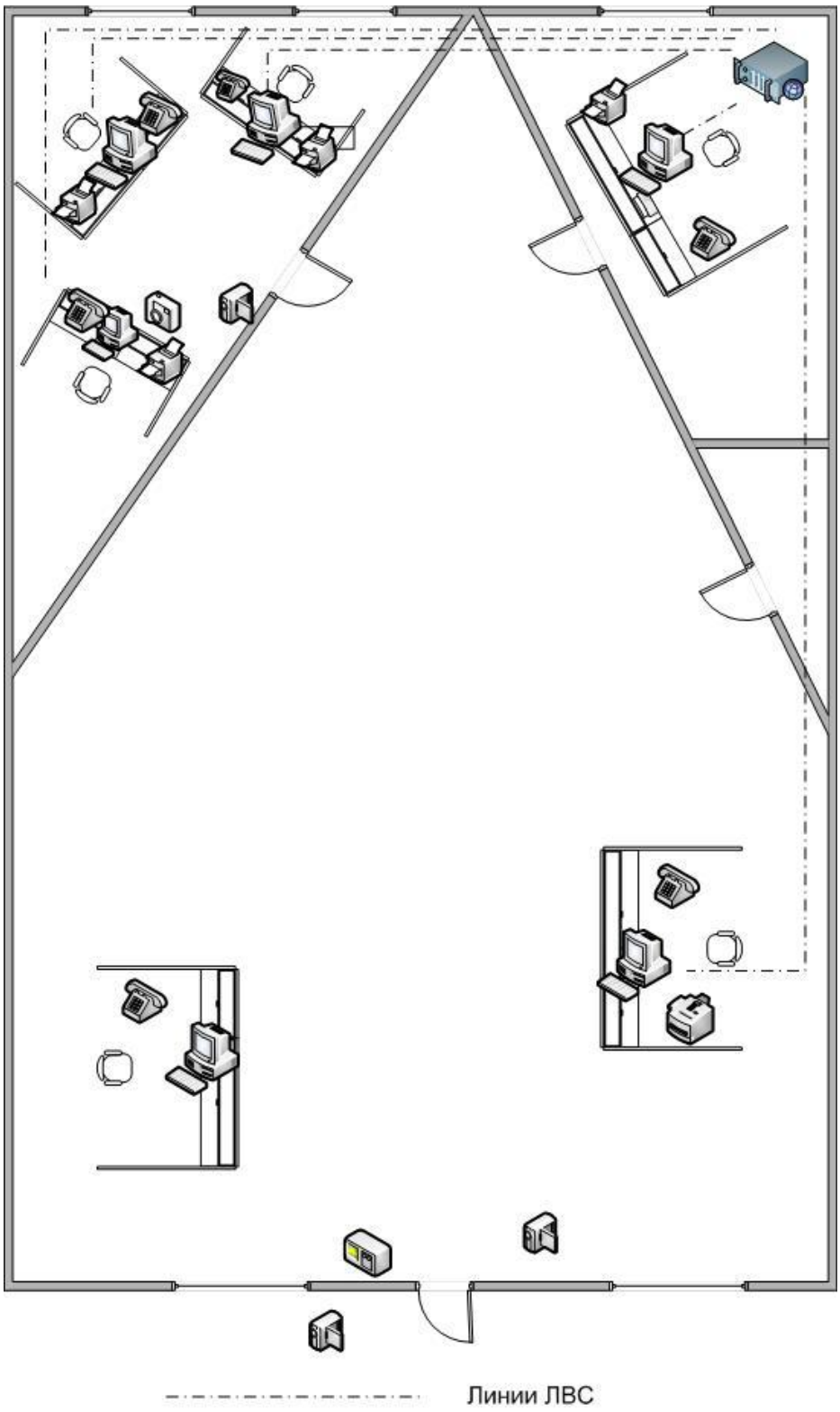

Рисунок 2.5 - Размещение линий локально-вычислительной сети

2.6 Размещение линий охранно-пожарной системы приведено на рисунке 2.6.

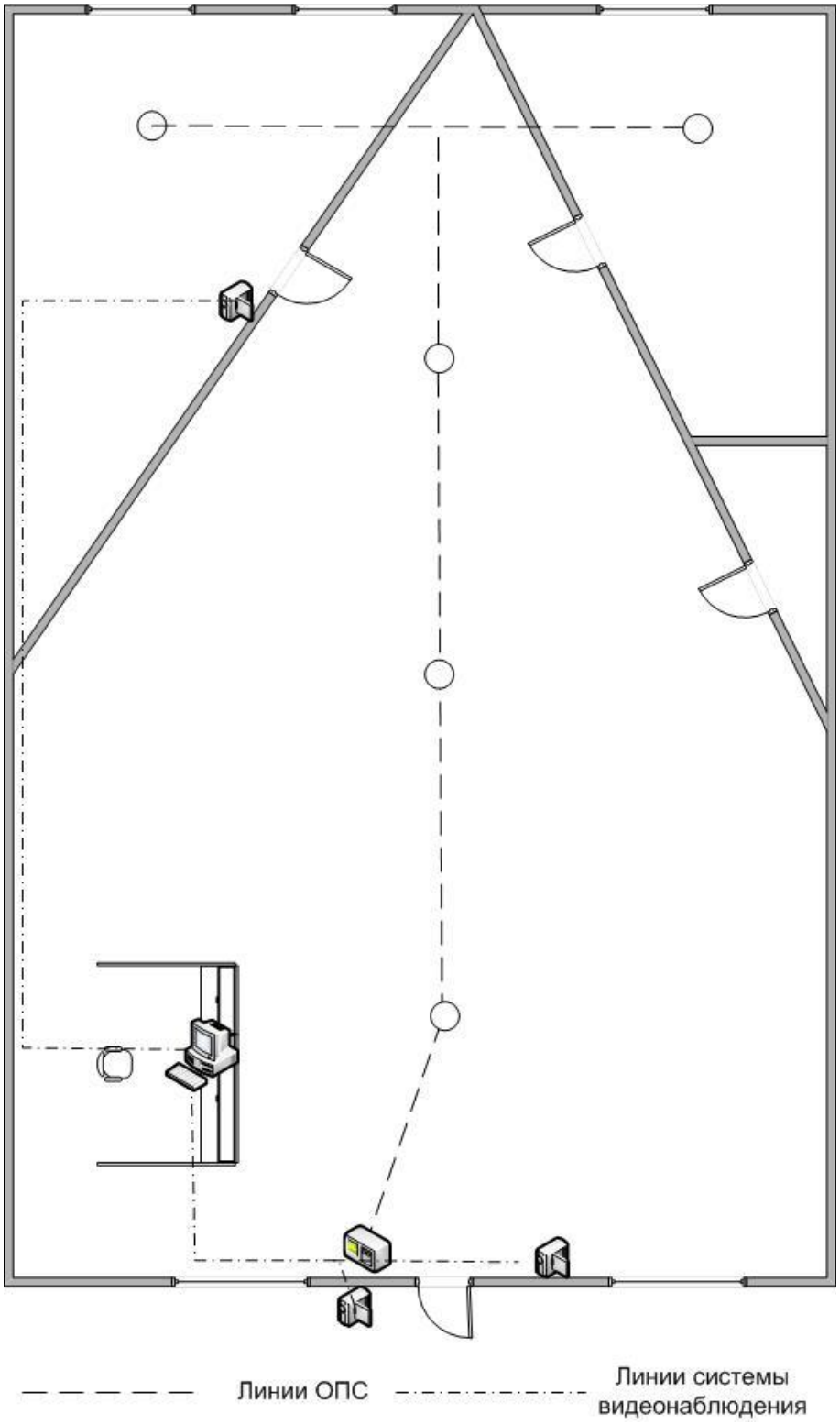

Рисунок 2.6 - Размещение линий охранно-пожарной системы

2.7 Размещение системы электропитания приведено на рисунке 2.7.

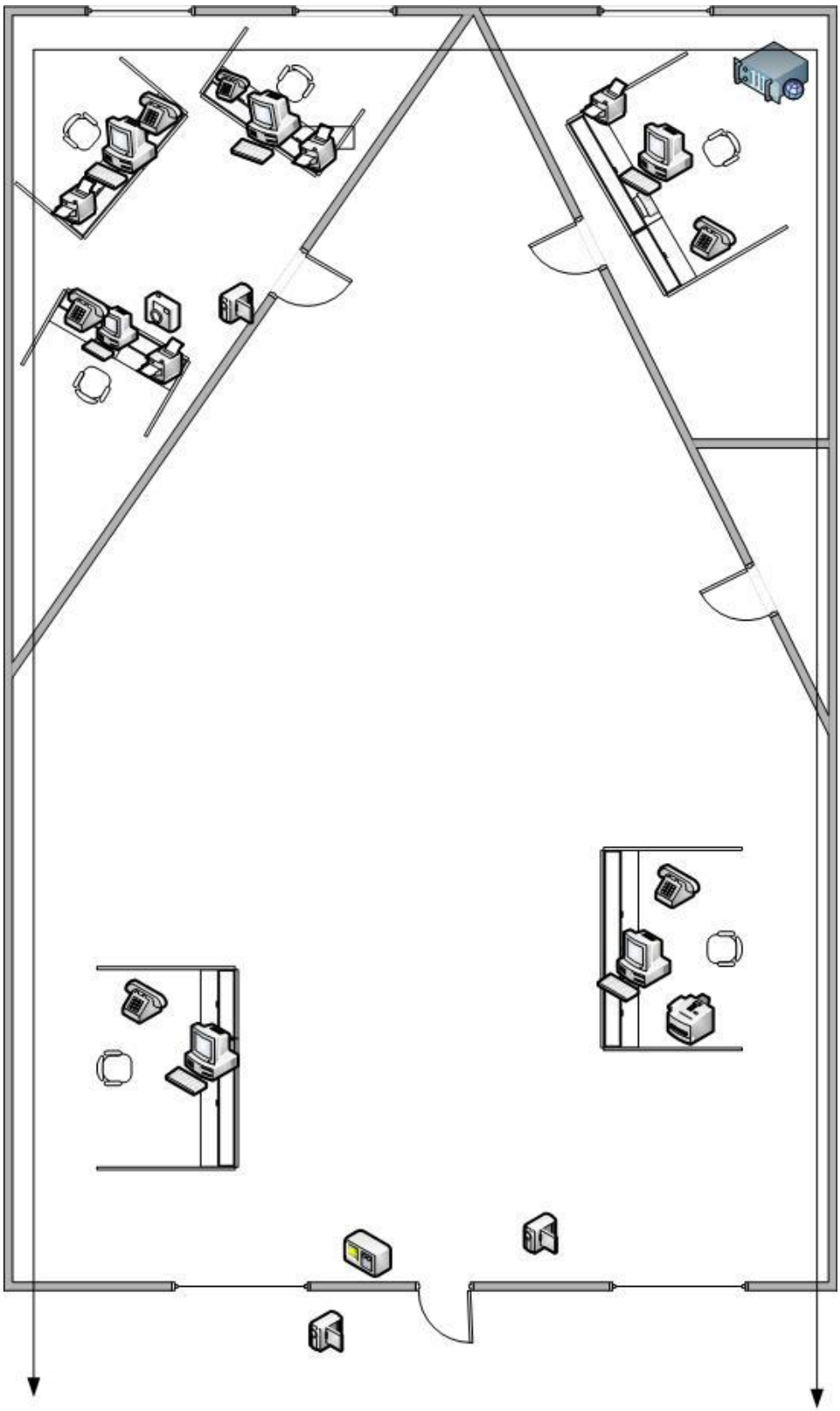

Рисунок 2.7 – Размещение системы электропитания

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

2.8 Перечень средств защиты информации, установленных на объекте информатизации ИСПДн «КЛИЕНТЫ БАНКА» приведен в Таблице 2.3.

Таблица 2.3 – Перечень средств защиты, установленных на ОИ ИСПДн «КЛИЕНТЫ БАНКА»

Наименование и тип технического средства	Заводской номер/СЗЗ	Сведения о сертификате	Расположение
Антивирусное ПО «Kaspersky Endpoint Security 10 для Windows»		№ 3025 действ. до 25.11.2020 г.	В ПЭВМ
МЭ Cisco ASA5510		№213 действ. До 19.03.2021г.	В кабинете руководителя

2.9 Перечень программных средств, установленных на объекте информатизации ИСПДн «КЛИЕНТЫ БАНКА» приведен в Таблице 2.4.

Таблица 2.4 – Перечень ПО установленного на ОИ ИСПДн «КЛИЕНТЫ БАНКА»

Наименование ПО	Версия
Microsoft Windows 10	1703
7-zip	9.20.00.0
Kaspersky Endpoint Security 10 для Windows	10.2.5.3201
Операционный день банка	3.1
1С: Предприятие 1С: Бухгалтерия	8
Microsoft office 365	

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 дополнительного

офиса №5 АО«УРАЛПРОМБАНК »

_____В.Э. Гогель

«___» _____2018 г.

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на модернизацию системы защиты персональных данных на предприятии АО «УРАЛПРОМБАНК»

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

Полное наименование системы: Система защиты информационной системы обработки персональных данных, в акционерном обществе «УРАЛПРОМБАНК»

1.2. Наименование заказчика и исполнителя

Предприятие разработчик системы: АО «УРАЛПРОМБАНК», в лице специалиста по защите информации.

Предприятие заказчик системы: АО «УРАЛПРОМБАНК», в руководителя дополнительного офиса №5.

1.3. Перечень документов, на основании которых модернизируется система:

– 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;

– Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

1.4. Порядок оформления и предъявления заказчику результатов работ по модернизации 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 и/или предварительных проектов. Окончательный вариант проекта предоставляется на рассмотрение заказчику после специалиста по защите информации АО «УРАЛПРОМБАНК».

2. НАЗНАЧЕНИЕ И ЦЕЛИ МОДЕРНИЗАЦИИ СИСТЕМЫ

2.1. Назначение модернизации системы

В связи с введением нового рабочего места и добавлением фото клиентов в базу данных.

2.2. Цели модернизации системы

Основной целью проведения работ является приведение всех этапов работы с информации в информационной системе обработки персональных данных АО «УРАЛПРОМБАНК» в соответствие требованиям перечисленных в данном Техническом задании.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

Объектом защиты является ИСПДн «КЛИЕНТЫ БАНКА» включающая в себя:

1. Автоматизированные рабочие места:
   - АРМ руководителя
   - АРМ секретаря
   - 3 АРМ кассиров-операционистов
2. Помещения для хранения и работы с важной защищаемой информацией:
   - помещение дополнительного офиса №5.
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:
   - 5 мониторов АРМ;
   - 3 принтера HP LaserJet 1018;
   - МФУ HP LaserJet Pro.
5. Система бесперебойного питания АРМ:
   - источник бесперебойного питания АРМ руководителя;
   - источник бесперебойного питания АРМ секретаря;
   - источник бесперебойного питания 3 АРМ кассиров-операционистов.
6. Носители информации:
   - бумажные носители информации ограниченного доступа;
   - электронные (CD/DVD диски, флэш-накопители с документами, содержащими информацию ограниченного доступа);
   - персонал.
7. Персонал:
   - руководитель;
   - секретарь;
   - 3 кассира-операциониста.

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:

- уничтожение информации в случае повреждения носителей информаци;
- несанкционированный доступ к информации в системе, хранящейся на АРМ.

3.2.2. Присутствуют следующие уязвимости:

3.2.2.1. АРМ:

- отсутствие инструкции по эксплуатации СЗИ;

– неактуальность актов категорирования и классификации объекта информатизации.

4. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО МОДЕРНИЗАЦИИ СИСТЕМЫ

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 уровня защищённости ИСПДн, инструкции по эксплуатации СЗИ, технического паспорта;

– изучение существующих организационных мер обеспечения безопасности информации ограниченного доступа;

– разработка актуализированной модели угроз;

– разработка перечня требований по защите информации ограниченного доступа;

– 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 ИСПДн:

– 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;

– обновление программных продуктов информационной системы до актуального состояния.

4.3. Порядок проведения работ:

4.3.1. 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 ГОТОВОЙ СИСТЕМЫ

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 ПЕРСОНАЛЬНЫХ ДАННЫХ 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 модернизации системы исполнителем должны быть подготовлены следующие документы:

– Программа и методика испытаний объекта информатизации;
– Определения уровня защищенности;
– Технический паспорт.

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 дополнительного офиса №5 АО «УРАЛПРОМБАНК»

_____В.Э. Гогель

«____»_____ 2018 г.

ПЕРЕЧЕНЬ ПЕРСОНАЛЬНЫХ ДАННЫХ,
подлежащих защите в информационной системе обработки персональных данных ИСПДн «КЛИЕНТЫ БАНКА»

№	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.	Номер телефона
7.	Фото

Руководитель дополнительного офиса №5 АО «УРАЛПРОМ-БАНК» _____ В.Э. Гогель

ПРИЛОЖЕНИЕ Г

УТВЕРЖДАЮ

Руководитель дополнительного офиса №5 АО «УРАЛПРОМБАНК»

_____В.Э. Гогель

«____» _____ 2018 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
в информационной системе обработки персональных данных
ИСПДн «КЛИЕНТЫ БАНКА»

2018 г.

УСЛОВНЫЕ СОКРАЩЕНИЯ:

АВЗ – антивирусная защита;

ИСПДн – информационная система персональных данных;

ПДн – персональные данные.

1 ОБЩИЕ ТРЕБОВАНИЯ

1.1. Настоящая инструкция определяет требования к организации защиты информационной системы обработки персональных данных ИСПДн «КЛИЕНТЫ БАНКА» АО «УРАЛПРОМБАНК» (далее ИСПДн) от разрушающего воздействия компьютерных вирусов и иного вредоносного программного обеспечения и устанавливает ответственность руководителя и сотрудников, эксплуатирующих и сопровождающих ИСПДн, за их выполнение.

1.2. К использованию в ИСПДН допускаются только лицензионные антивирусные средства, централизованно закупленные у разработчиков (поставщиков) указанных средств.

1.3. Установка и настройка средств антивирусного контроля на рабочих станциях ИСПДн осуществляется администратором или специально назначенным лицом в соответствии с руководствами по применению конкретных антивирусных средств.

1.4. Данные требования не распространяются на рабочие станции с установленными операционными системами, для которых отсутствуют какие-либо средства антивирусного контроля.

2 ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

2.1. Любой программный модуль перед запуском должен проходить автоматический антивирусный контроль. Для этого необходимо осуществлять проверку либо при загрузке компьютера всех дисков и файлов рабочих станций, либо непосредственно перед запуском конкретного программного модуля.

2.2. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных носителях (магнитных дисках, оптических и т.п.). Разархивирование и контроль входящей информации необходимо проводить непосредственно после ее приема на выделенном автономном компьютере. Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съемный носитель).

2.3. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера (локальной вычислительной сети), администратором защиты ИСПДн должна быть выполнена антивирусная проверка на защищаемых серверах и рабочих станциях.

2.4. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник подразделения самостоятельно или вместе с администратором защиты ИСПДн должен провести внеочередной антивирусный контроль своей рабочей станции.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов пользователи ИСПДн обязаны:

- приостановить работу в ИСПДн;

- немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя подразделения и администратора защиты ИСПДн, владельца зараженных файлов, а также смежные подразделения, использующие эти файлы в работе;
- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- провести лечение или уничтожение зараженных файлов.

3 ОТВЕТСТВЕННОСТЬ

3.1. Ответственность за организацию и проведение антивирусного контроля в соответствии с требованиями настоящей Инструкции возлагается на администратора соответствующей информационной системы персональных данных.

3.2. Периодический контроль состояния антивирусной защиты в ИСПДн, а также соблюдения установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции осуществляется администратором за обеспечение безопасности персональных данных.

Руководитель дополнительного офиса №5
АО «УРАЛПРОМБАНК» _____ В.Э. Гогель

С инструкцией ознакомлены:

№	ФИО	Подпись
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15.		
16.		
17.		
18.		
19.		

ПРИЛОЖЕНИЕ Д

«УральскийПромышленныйБанк»
Акционерное общество «УРАЛПРОМБАНК»
Адрес 454090 г. Челябинск. Свободы,97
Тел: (351) 263-08-75
Эл. Почта:post@uralprombank.ru www.uralprombank.ru
ИНН/КПП: 7449014065/745301001

УТВЕРЖДАЮ
Руководитель дополнительного офиса №5 АО «УРАЛПРОМБАНК»
_____
_____2018 г.

АКТ

от _____ 2018 г. №

г. Коркино

определения уровня защищенности персональных данных информационной системы персональных данных «КЛИЕНТЫ БАНКА»

Составлен комиссией
Председатель:
1. Руководитель _____
Члены комиссии
2. Специалист по ИБ _____
3. Специалист по ИБ _____
4. Специалист по ИБ _____

Руководствуясь Постановлением Правительства от 01.11.12 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», комиссия установила, что:

- ИСПДн является системой, обрабатывающей **биометрические персональные данные;**
- в ИСПДн обрабатываются персональные данные субъектов, **не являющимися работниками организации**;
- актуальными являются угрозы **3-го типа.**

Установив исходные данные, комиссия определила, что для персональных данных ИСПДн необходимо определить уровень защищенности **3.**

ПРИЛОЖЕНИЕ Е

УТВЕРЖДАЮ
Руководитель дополнительного офиса №5 АО «УРАЛПРОМБАНК»

_____В.Э. Гогель
«____» _____ 2018 г.

ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ
в информационной системе обработки персональных данных
«КЛИЕНТЫ БАНКА»

2018 г.

Продолжение приложения Е

1.Общие положения

1.1 Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах персональных данных (далее – ИСПДн), а также контроль за действиями пользователей и обслуживающего персонала системы при работе с паролями.

1.2 Требования настоящей инструкции являются обязательными для исполнения всеми пользователями ИСПДн, а также другими сотрудниками, использующими в своей работе средства вычислительной техники.

1.3 Весь личный состав должен быть ознакомлены с требованиями Инструкции под роспись.

1.4 Контроль за выполнением требований Инструкции возлагается на ответственного за обеспечение безопасности персональных данных.

1.5 Настоящая Инструкция является дополнением к действующим нормативным документам по вопросам защиты информации и не исключает обязательного выполнения их требований.

2. Организация парольной защиты

2.1. Парольная защита применяется для решения следующих задач:
— обеспечение защиты информационных ресурсов информационных систем персональных данных от непреднамеренного воздействия, несанкционированного воздействия, разглашения, утечки, а также хищения, утраты, уничтожения, искажения или подделки за счет специальных воздействий;
— предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных закладок;
— защита информации ограниченного распространения (защита персональных данных).

2.2. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах ИСПДн и контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями возлагается на ответственного за обеспечение безопасности персональных данных.

3. Требования, предъявляемые к паролю

3.1. Личные пароли должны генерироваться и распределяться централизованно либо выбираться пользователями системы самостоятельно с учетом следующих требований:
— пароль сотрудником выбирается самостоятельно (при самостоятельном выборе пароля пользователем);
— пароль должен знать только его владелец (при самостоятельном выборе пароля пользователем);
— пароль сотрудник вводит собственноручно (при самостоятельном выборе пароля пользователем);
— длина пароля должна быть не менее 6 символов;
— должна быть соблюдена сложность пароля (в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры);

— пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER и т.п.);

— при смене пароля новое значение должно отличаться от предыдущего не менее чем в 4 позициях;
— личный пароль пользователь не имеет права сообщать никому.

3.2. Полная плановая смена паролей пользователей должна проводиться регулярно, не реже одного раза в 90 дней.

3.3. В случае компрометации личного пароля пользователя ИСПДн должна быть немедленно произведена внеплановая смена пароля в присутствии ответственного за обеспечение безопасности персональных данных.

3.4. Хранение сотрудником значений своих паролей на бумажном носителе допускается только в личном, опечатанном владельцем пароля сейфе, либо в сейфе у ответственного за обеспечение безопасности персональных данных или начальника отдела в опечатанном личной печатью пенале (возможно вместе с персональными идентификаторами).

3.5. Повседневный контроль за действиями исполнителей и обслуживающего персонала системы при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на ответственных за информационную безопасность (руководителей подразделений), периодический контроль возлагается на ответственного за обеспечение безопасности персональных данных.

4. Ответственность

4.1. Пароль является служебной тайной, и каждый сотрудник несет ответственность за сохранность в тайне собственного пароля в соответствии с действующим законодательством.

4.2. В случае генерировании пароля и его централизованном распределении ответственность за сохранность пароля несут ответственный за обеспечение безопасности персональных данных и пользователь, которому выдан пароль.

Руководитель дополнительного офиса №5
АО «УРАЛПРОМБАНК» В.Э. Гогель

№	ФИО	Подпись
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		
11.		
12.		
13.		
14.		
15		
16.		
17.		
18.		
19.		

ПРИЛОЖЕНИЕ Ж

Информационное письмо о внесении изменений в сведения в реестре операторов, осуществляющих обработку персональных данных

Наименование оператора: "Уральский Промышленный Банк" (открытое акционерное общество)

Адрес местонахождения: 454090, г. Челябинск, ул. Свободы, д. 97

Контактная информация оператора:
телефон: 8-351-908-20-08
адрес электронной почты: post@uralprombank.ru
Регионы: Челябинская область
ИНН: 7449014065

Регистрационный номер записи в Реестре: 09-0038917
Основания изменений: внесение изменений в перечень категории персональных данных

Филиалы:
Дополнительный офис №1, Челябинск, Комсомольский проспект, д. 111
Дополнительный офис №4, Челябинск, ул. Гагарина, 9а
Дополнительный офис №5, Чел. обл., г. Коркино**,** ул. Мира, д. 35

Правовое основание обработки персональных данных
следующими нормативно-правовыми актами: Конституция Российской Федерации от 25.12.1993; Гражданский кодекс Российской Федерации от 30.11.1994 № 51-ФЗ; Трудовой кодекс Российской Федерации от 30.12.2001 N 197-ФЗ; Уголовный кодекс Российской Федерации от 13 июня 1996 г. N 63-ФЗ; Кодекс Российской Федерации об административных правонарушениях от 30 декабря 2001 г. N 195-ФЗ; Налоговый Кодекс Российской Федерации часть первая от 31 июля 1998 г. N 146-ФЗ и часть вторая от 5 августа 2000 г. N 117-ФЗ; Федеральный закон от 02.12.1990 №395-1 «О банках и банковской деятельности»; Федеральный закон от 07.08.200 №115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»; Федеральный закон от 30.12.2004 N 218-ФЗ «О кредитных историях»; Федеральный закон от 10.12.2003 N 173-ФЗ «О валютном регулировании и валютном контроле»; Федеральный закон от 22.04.1996 N 39-ФЗ «О рынке ценных бумаг»; Федеральный закон от 25.02.1999 N 40-ФЗ «О несостоятельности (банкротстве) кредитных организаций»; Федеральный закон от 23.12.2003 N 177-ФЗ «О страховании вкладов физических лиц в банках Российской Федерации»; Федеральный закон от 27.07.2010 N 224-ФЗ «О противодействии неправомерному использованию инсайдерской информации и манипулированию рынком и о внесении изменений в отдельные законодательные акты Российской Федерации»; Федеральный закон от

19 декабря 2005 г. N 160-ФЗ «О ратификации Конвенции Совета Европы «О защите физических лиц при автоматизированной обработке персональных данных»; Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и защите информации»; Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»; Указ Президента РФ от 6 марта 1997 г. N 188 «Об утверждении Перечня сведений конфиденциального характера»; Постановление Правительства РФ от 15.09.2008 N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»; Постановление Правительства РФ от 17 ноября 2007 г. N 781 «Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»; Постановление Правительства РФ от 06.07.2008 N 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»; Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. N 55/86/20 «Об утверждении Порядка проведения классификации информационных систем персональных данных»; Приказ ФСТЭК России от 5 февраля 2010 г. №58 «Об утверждении Положения о методах и способах защиты информации в информационных системах персональных данных»; Устав АО «УРАЛПРОМБАНК» (утвержден общим собранием акционеров от 7 апреля 2006 года).

Цель обработки персональных данных:

предоставления банковских услуг физическим и юридическим лицам (операции с расчетными счетами юридических лиц и индивидуальных предпринимателей, операции с вкладами, денежные переводы, операции с банковскими картами, выдача кредитов, аренда ячеек, продажа монет, покупка ценных бумаг, зарплатные проекты, прием платежей, обмен валюты, система дистанционного банковского обслуживания (Интернет-Банк)), осуществления трудовых (договорных) отношений.

Описание мер, предусмотренных статьями 18.1. и 19 Федерального закона «О персональных данных»:

Назначение ответственного за организацию обработки персональных данных; 2. Издание документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений; 3. Применение правовых, организационных и технических мер по обеспечению безопасности персональных данных; 4. Осуществление внутреннего контроля соответствия обработки персональных данных требованиям законодательства; 5. Ознакомление работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных; 6. Определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

7. Применение прошедших в установленном порядке процедуру оценки соответствия средств защиты информации; 8.Учет машинных носителей персональных данных; 9. Обнаружение фактов несанкционированного доступа к персональным данным и принятие мер; 10. Восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним; 11. Установление правил доступа к персональным данным, обрабатываемым в информационной системе персональных данных, а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных; 12. Контроль за принимаемыми мерами по обеспечению безопасности персональных данных.

Средства обеспечения безопасности: используются антивирусные средства защиты информации, идентификация и проверка подлинности пользователя при входе в информационную систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов; наличие средств восстановления системы защиты персональных данных.

Сведения об обеспечении безопасности персональных данных в соответствии с требованиями к защите персональных данных, установленными Правительством РФ: Определены места хранения персональных данных (материальных носителей). Определен перечень лиц, осуществляющих обработку персональных данных и имеющих к ним доступ. Обеспечено раздельное хранение персональных данных (материальных носителей), обработка которых осуществляется в различных целях. Обеспечен учет материальных носителей. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, учтены в соответствующих журналах. Исключена возможность неконтролируемого проникновения или пребывания посторонних лиц в помещения, где ведется работа с персональными данными. Обеспечена сохранность носителей персональных данных и средств защиты информации.

Дата начала обработки персональных данных: 26.06.1991

Срок или условие прекращения обработки персональных данных: утрата правовых оснований обработки персональных данных

Сведения об информационной системе № 1:

Категории персональных данных

осуществляет обработку следующих категорий персональных данных:

биометрические персональные данные, фамилия, имя, отчество, год рождения, месяц рождения, дата рождения, место рождения, адрес, семейное положение, социальное положение, имущественное положение, образование, профессия, доходы; ИНН; СНИЛС (№ страхового пенсионного свидетельства); табельный номер;

номер, дата трудового договора; наименование и степень знания иностранного языка; наименование образовательного учреждения; стаж работы; состояние в браке; состав семьи, с указанием степени родства, фамилии, имени, отчества, года рождения, адреса места жительства ближайших родственников; данные документа, удостоверяющего личность (вид, серия, номер, дата выдачи, наименование органа, выдавшего документ); телефон; сведения о воинском учете (категория запаса, воинское звание, состав (профиль), полное кодовое обозначение ВУС; категория годности к военной службе, наименование военного комиссариата по месту жительства, состоит на воинском учете, отметка о снятии с учета) дата приема на работу; характер работы; вид работы (основной, по совместительству); структурное подразделение; занимаемая должность (специальность, профессия), разряд, класс (категория) квалификации; ранее занимаемая должность; тарифная ставка (оклад), надбавка, руб. основание трудоустройства; личная подпись сотрудника; фотография; сведения об аттестации (дата, решение, номер и дата документа, основание); сведения о профессиональной подготовке (дата начала и окончания переподготовки, специальность (направление, профессия, наименование, номер, дата документа свидетельствующего о переподготовке, основание переподготовки); сведения о наградах, поощрениях, почетных званиях (наименование, номер, дата награды); сведения об отпусках (вид, период работы, количество дней, дата начала и окончания, основание); сведения о социальных льготах, на которые работник имеет право в соответствии с законодательством (наименование льготы, номер, дата выдачи документа, основание); сведения об увольнении (основания, дата, номер и дата приказа); объем работы; повышение оклада за вредность в %, в руб; месячный фонд ЗПЛ (в т.ч. по должностному окладу и районным коэффициентом); надбавка за стаж в %, в руб. в г/м/д; национальность; сведения о предыдущих фамилии, имени, отчестве; гражданство; уровень владения иностранными языками; сведения о судимостях; сведения о пребывании за границей; сведения о предыдущих местах работы; сведения о третьих лицах (родственники, работодатели, поручители); совершение финансовых операций (платежи, кредиты, пр.), состояние банковских счетов, контактная информация (телефоны, электронный адрес), вид запрашиваемого кредита, порядок гашения кредита, пол, количество иждивенцев, наличие заграничного паспорта, наличие водительского удостоверения, водительский стаж, сведения о переездах за последние 10 лет, наличие брачного контракта, недвижимость, автотранспорт, ценные бумаги, прочее имущество, находящееся в семейной собственности, дополнительная информация, которую субъект желает сообщить о себе.

Категории субъектов, персональные данные которых обрабатываются

принадлежащих: работникам, состоящим в трудовых отношениях с АО «УРАЛПРОМБАНК», физическим лицам: заёмщикам, вкладчикам и другим субъектам, состоящим в договорных и иных гражданско-правовых отношениях с АО «УРАЛПРОМБАНК», поручителям а также лицам, обработка персональных данных которых необходима в целях заключения договора.

Перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных: сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передача (распространение, предоставление, доступ), блокирование, удаление, уничтожение персональных данных.

Обработка вышеуказанных персональных данных будет осуществляться путем: смешанная, с передачей по внутренней сети юридического лица, с передачей по сети Интернет.

Осуществление трансграничной передачи персональных данных: не осуществляется .

Ответственный за организацию обработки персональных данных: Емельянов Антон Александрович, 8-351-908-20-08; eaa@uralprombank.ru.