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

Высшая школа электроники и компьютерных наук

Кафедра «Защита информации»

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

Защита автоматизированной системы обработки персональных данных в ООО МФО "Городской Займ"

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
К ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЕ

Автор проекта,
студент группы КЭ- 431
_____ Курмантаева, А. З.
_____ 2017 г.

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

Челябинск 2017

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И ОПРЕДЕЛЕНИЯ

ООО - Общество с ограниченной ответственностью;
МФО - микрофинансовая организация;
АС - автоматизированная система;
ИБ - информационная безопасность;
ИТ - информационные технологии;
ЗИ - защита информации;
АРМ - автоматизированное рабочее место;
ПДн - персональные данные;
СЗИ – средство защиты информации;
НСД - несанкционированный доступ;
ИСПДн - информационная система персональных данных;
ОС - операционная система;
ПО - программное обеспечение;
РФ - Российская Федерация;
ФСБ - Федеральная служба безопасности;
ФСТЭК - Федеральная служба по техническому и экспортному контролю
ФЗ - Федеральный Закон.

Автоматизированная система - система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.[1, с. 6]

Информационная система персональных данных - это информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.[1, с. 7]

Несанкционированный доступ - доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своим функциональному предназначению и техническим характеристикам.[1, с.7]

Персональные данные - любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.[1, с. 8]

Утечка (защищаемой) информации по техническим каналам - неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.[1,с. 9]

Уязвимость - некая слабость, которую можно использовать для нарушения системы или содержащейся в ней информации.[1, с. 9]

ВВЕДЕНИЕ

Актуальность темы данной выпускной квалификационной работы обусловлена тем, что защита персональных данных для любой из современных организаций является одной из значимых задач в ее деятельности. С развитием информационных технологий возрастает и ужесточается количество требований к информационной безопасности, что ведет за собой потребность в постоянном совершенствовании существующих мер по защите информации.

Разработка и реализация проекта, направленного на повышение качества системы защиты персональных данных, позволит повысить общий уровень информационной безопасности организации.

Объектом выпускной квалификационной работы является ООО МФО «Городской Займ».

Предметом работы является существующая автоматизированная система обработки персональных данных «Клиенты».

Целью данной работы является создание эффективного комплекса мер по защите автоматизированной системы обработки персональных данных в ООО МФО «Городской Займ».

Для достижения цели были поставлены следующие задачи:

1. Провести анализ состояния защиты информации в ООО МФО «Городской Займ» и выявить существующие проблемы;
2. Проанализировать и теоретически обосновать выбор средств защиты персональных данных;
3. Разработать проект системы защиты персональных данных в ООО МФО «Городской Займ».

ГЛАВА 1 АНАЛИЗ СОСТОЯНИЯ ЗАЩИТЫ ИНФОРМАЦИИ В ООО МФО «ГОРОДСКОЙ ЗАЙМ» И СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ

1.1. Разработка паспорта организации с точки зрения информационной безопасности в ООО МФО «Городской Займ»

Для формирования общего представления об объекте выпускной квалификационной работы был составлен паспорт организации с точки зрения информационной безопасности. Паспорт организации с точки зрения информационной безопасности представлен в Приложении А.

Паспорт предприятия с точки зрения информационной безопасности составлен на основе информации, полученной от директора и сотрудников организации. В нем содержится описание структуры, информационной среды, а также сведения о наличии лицензий и реквизиты организации.

Полученная информация необходима для описания информационной системы, разработки модели деятельности защищаемого объекта, а также модели угроз и уязвимостей организации.

В качестве защищаемого объекта был выбран отдел по работе с клиентами ООО МФО «Городской Займ».

1.2. Разработка модели деятельности ООО МФО «Городской Займ»

Разработанная модель деятельности отдела по работе с клиентами представлена в приложении Б. Модель отражает базовые и вспомогательные бизнес-процессы отдела.

Необходимость построения данной модели состоит в наглядном представлении деятельности отдела данной организации и выявлении циркулирующей в нем информации. В модели описаны этапы работы по предоставлению потребительских кредитов, что является базовым бизнес-процессом ООО МФО «Городской Займ». Кроме того, модель деятельности может быть использована в качестве наглядного примера при проведении соответствующих мероприятий по обучению персонала, изменении текущих бизнес-процессов и описания взаимодействия объектов, требующих защиту, с другими объектами в организации.

1.3. Выявление защищаемой информации в ООО МФО «Городской Займ»

Защищаемой информацией является такая информация, что подлежит защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.[3, с. 2]

В процессе анализа деятельности и организационно-распорядительной документации отдела по работе с клиентами ООО МФО «Городской Займ» была выявлена защищаемая информация. Защищаемой информацией являются сведения, составляющие персональные данные (на основании Федерального Закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»).

Разработанная в рамках выпускной квалификационной работы Политика в отношении обработки персональных данных представлена в Приложении В.

Акт определения необходимого уровня защищенности персональных данных, обрабатываемых в ИСПДн «Клиенты» представлен в Приложении Г.

1.4. Описание информационной системы ООО МФО «Городской Займ»

Безопасность информационной системы ООО МФО «Городской Займ» реализуется по средствам внедрения организационных, технических и программно-аппаратных средств обработки и хранения защищаемой информации. Рассмотрим их подробнее:

1. В качестве организационных средств используются такие документы как:
   - Должностные инструкции персонала;
   - Положение об обработке и защите ПДн;
   - Обязательство о неразглашении ПДн работников и клиентов;
   - Перечень сотрудников организации, ответственных за обработку ПДн;
   - План произведения проверок на соблюдение требований Положения;
   - Лист ознакомления с локальными НПА.

2. Среди правовых средств можно выделить действующие в организации документы, такие как:
   - Трудовой кодекс Российской Федерации;
   - Гражданский кодекс Российской Федерации;
   - Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
   - Федеральный закон от 27 июля 2006 г. N 152-ФЗ «О персональных данных»;
   - Приказ ФСТЭК России N 21 от 18 февраля 2013 г. «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
   - Постановление Правительства РФ от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
   - Постановление Правительства РФ от 15 сентября 2008 г. N 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
   - Комплекс документов Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».

3. Для описания программно-аппаратных средств ООО МФО «Городской Займ» потребовалось провести инвентаризацию системы.

Перечень программных средств представлен в таблице 1, перечень аппаратных средств представлен в таблице 2.

Таблица 1 – Программное обеспечение.

Наименование	Назначение	Версия
Microsoft Windows 7	Операционная система	8.15.10.2141 (SP1)
Microsoft Office 2007	Пакет программ, используемый для работы с документацией	12.0.4518.1014
Microsoft Security Essentials	Антивирусное ПО	4.9.218.0
Кредитный инспектор	ПО для автоматизации процесса выдачи займов	17.31

Таблица 2 – Аппаратное обеспечение.

Наименование	Характеристики	Заводской номер
АРМ		
Системный блок DEXP Aquilon O126	Pentium J2900, 2410 МГц, 2 ГБ, 500 ГБ, Ethernet	Инв. № 1357908
Монитор LG 22M38A-B	21.5", 1920x1080, VGA	Инв. № 1358809
Клавиатура DEXP K-503BU	проводная, USB, 104 клавиши	Инв. № 1368933
Мышь DEXP CM-408BU	800 dpi, оптическая светодиодная, USB	Инв. № 1356879
Принтер Samsung SL-C430	2400x600 dpi, ч/б - 18 стр/мин (A4), USB	Инв. № 1384524

1.5. Выявление объектов защиты ООО МФО «Городской Займ»

В ходе анализа процессов, средств и методов обработки информации в организации были выявлены объекты защиты. Также, в процессе выявления был задействован перечень защищаемой информации, в качестве обоснования выбора.

Выявленные объекты защиты:

- АРМ сотрудников;
- средства ввода и вывода информации;
- носители информации;
- помещение для хранения и обработки защищаемой информации.

1.6. Разработка модели угроз и уязвимостей для объектов защиты ООО МФО «Городской Займ»

Разработка модели угроз и уязвимостей необходима для определения дальнейших мероприятий по защите информации.

Для того чтобы разработать модель угроз и уязвимостей для объектов защиты, нужно, прежде всего, определить защищаемые объекты. Определим их исходя из

перечня защищаемой информации – критически важными объектами будут считаться те, при помощи которых обрабатываются и хранятся ПДн:

- АРМ сотрудника;
- носители информации.

Проанализировав «Базовую модель угроз безопасности информации при их обработке в ИСПДн» ФСТЭК России от 15 февраля 2008 г. был составлен перечень возможных угроз безопасности персональных данных. Учитывая особенности ИСПДн ООО МФО «Городской Займ», возможна реализация следующих угроз:

- угроз утечки информации по техническим каналам;
- угроз НСД к ПДн, обрабатываемым на автоматизированном рабочем месте.

Исходя из этого перечня, определим уязвимости:

- отсутствие организационно-распорядительных документов по ЗИ;
- незнание или игнорирование сотрудниками организационных требований;
- отсутствие необходимых средств защиты на АРМ.

1.7. Расчет рисков важных объектов защиты ООО МФО «Городской Займ»

Расчет рисков информационной безопасности важных объектов защиты основан на документе Федеральной службы по техническому и экспортному контролю от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

Для оценки возможности реализации угрозы применяются следующие: уровень исходной защищенности ИСПДн «Клиенты» и частота (вероятность) реализации рассматриваемой угрозы.

1) Уровень исходной защищенности ИСПДн:

Чтобы определить исходную степень защищенности, нужно выявить показатели исходной защищенности ИСПДн, зависящие от технических и эксплуатационных характеристик. Для данной организации показатели исходной защищенности представлены в таблице 3.

Таблица 3 – Показатели исходной защищенности ИСПДн.

Технические и эксплуатационные характеристики ИСПДн	Уровень защищенности		
	Высокий	Средний	Низкий
1	2	3	4
1. По территориальному размещению: - локальная ИСПДн, развернутая в пределах одного здания	+	-	-

Продолжение таблицы 3

1	2	3	4
2. По наличию соединения с сетями общего пользования: - физически отделенная от сети общего пользования	+	-	-
3. По встроенным операциям с записями баз ПДн: - запись, удаление, сортировка	-	+	-
4. По разграничению доступа к ПДн: - ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации	-	+	-
5. По наличию соединений с другими базами ПДн иных ИСПДн: - ИСПДн, в которой используется одна база ПДн	+	-	-
6. По уровню обобщения ПДн: - ИСПДн, в которой данные обезличиваются только при передаче в другие организации	-	+	-
7. ПО объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки: - ИСПДн, не предоставляющая никакой информации	+	-	-

Определим процентное соотношение характеристик.

Высокий уровень защищенности:

- не менее 70% характеристик ИСПДн соответствуют высокому уровню, а остальные - среднему.

Для этого суммируем положительные решения по первому столбцу: 4, что составляет 57% характеристик. Следовательно, данная ИСПДн не имеет высокого уровня защищенности.

Средний уровень защищенности:

- не менее 70% характеристик ИСПДн соответствуют уровню не ниже среднего, а остальные соответствуют низкому.

Для этого вычислим сумму положительных решений по первому и второму столбцу, к общему количеству решений: 7, что составляет 100%.

Следовательно, ИСПДн «Клиенты» имеет средний уровень защищенности, и дальнейшее рассмотрение низкого уровня защищенности является нецелесообразным.

Для дальнейшего анализа в соответствии с методикой поставим средней степени исходной защищенности в соответствие числовой коэффициент $Y_1 = 5$.

2) Частота (вероятность) реализации рассматриваемой угрозы:

Данный показатель определяется экспертным путем и характеризует собой вероятность реализации конкретной угрозы безопасности ПДн. В соответствии с

вербальными градациями данного показателя, результат работы представлен в таблице 4.

Таблица 4 – Вероятности реализации угроз.

Угроза	Вероятность реализации	Числовой коэффициент Y_2
Угроза утечки информации по техническим каналам	Маловероятно	0
Угроза НСД к ПДн, обрабатываемым в АРМ	Низкая вероятность	2

Используя данные таблицы 4, рассчитаем коэффициент реализуемости угрозы Y по формуле:

$$Y = \frac{Y_1 + Y_2}{20}$$

Для угрозы утечки информации по техническим каналам полученное значение равно 0,25. Следовательно, по вербальной интерпретации реализуемости угрозы, возможность реализации угрозы признается низкой.

Для угрозы НСД к ПДн, обрабатываемым в АРМ, полученное значение равно 0,35. Следовательно, возможность реализации данной угрозы признается средней.

Далее необходимо оценить опасность каждой угрозы. Значения вербального показателя опасности для рассматриваемой ИСПДн представлены в таблице 5.

Таблица 5 – Показатели опасности угроз.

Угроза	Показатель опасности
Угроза утечки информации по техническим каналам	Средняя опасность
Угроза НСД к ПДн, обрабатываемым в АРМ	Высокая опасность

Осуществим выбор из общего перечня угроз безопасности тех, которые относятся к актуальным для ИСПДн «Клиенты», в соответствии с правилами, приведенными в таблице 6 в соответствии с методикой.

Таблица 6 - Правила отнесения угрозы безопасности ПДн к актуальной.

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

В соответствии в приведенными правилами:
1) Угроза утечки информации по техническим каналам для ИСПДн «Клиенты» является неактуальной.
2) Угроза НСД к ПДн, обрабатываемым в АРМ, для ИСПДн «Клиенты» является актуальной.

Использовав данные исследования актуальности угроз ИСПДн ООО МФО «Городской Займ» возможно сформулировать организационно-технические требования по защите от несанкционированного доступа и осуществить выбор программных и технических средств защиты информации, которые могут быть применены при дальнейшей эксплуатации информационной системы персональных данных.

1.8. Разработка технического задания на создание системы защиты ИСПДн

На основе проведенного анализа ИСПДн и исходных данных необходимо разработать техническое задание на создание системы защиты информационной системы персональных данных ООО МФО «Городской Займ».

Процесс разработки основан на ГОСТ 34.602-89. «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

В соответствии со стандартом, ТЗ содержит следующие разделы:

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

Разработанное техническое задание представлено в Приложении Д.

ВЫВОДЫ ПО ПЕРВОЙ ГЛАВЕ

Глава 1 посвящена анализу состояния защиты информации в ООО МФО «Городской Займ» и определению существующих угроз информационной безопасности.

В ходе исследования был составлен паспорт предприятия, в котором отображена исходная информация об организации. Была составлена модель деятельности отдела по обслуживанию клиентов организации, принятого в качестве защищаемого объекта. На основании разработанной модели деятельности была выявлена информация ограниченного доступа – персональные данные. Проведен анализ информационной системы отдела с целью выявления объектов защиты.

Основываясь на перечне объектов защиты и «Базовой модели угроз безопасности информации при их обработке в ИСПДн» ФСТЭК России от 15 февраля 2008 г. была разработана модель угроз и уязвимостей. В соответствии с документом ФСТЭК России от 14 февраля 2008 г. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», был определен уровень защищенности ИСПДн – средний, а также вероятность реализации каждой из угроз. Уровень защищенности ПДн, в соответствии с постановлением правительства от 1 ноября 2012 г. N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», четвертый.

В результате анализа полученных данных, было составлено техническое задание на разработку информационной системы персональных данных ООО МФО «Городской Займ».

ГЛАВА 2 ТЕОРЕТИЧЕСКОЕ ОБОСНОВАНИЕ ВЫБОРА СРЕДСТВ ЗАЩИТЫ

2.1. Обзор возможных методов устранения уязвимостей

Проанализировав полученную модель угроз и уязвимостей ООО МФО «Городской Займ», необходимо провести обзор возможных методов их устранения.

Этот процесс является необходимым этапом в осуществлении выбора наиболее эффективного решения поставленных задач. В информационной системе организации обеспечение безопасности персональных данных является важнейшей задачей, поэтому следует рассмотреть каждую из угроз по отдельности и определить необходимые меры по устранению вероятных и существующих уязвимостей.

2.2. Угрозы, связанные с НСД

Угрозы несанкционированного доступа к персональным данным является актуальными для данной организации, даже при невысокой вероятности реализации, представляя собой опасность для ИСПДн.

ИСПДн «Клиенты» в ООО МФО «Городской Займ» является системой, обрабатывающей ПДн на автоматизированном рабочем месте, не имеющем подключения к сетям связи общего пользования и (или) сетям международного информационного обмена. Рассмотрим угрозы, связанные с НСД относительно данной информационной системы.

Источниками угроз несанкционированного доступа могут являться:

- внутренние (пользователи) и внешние нарушители;
- аппаратные закладки;
- носители вредоносных программ.

Реализация таких угроз происходит при осуществлении несанкционированного доступа, включающего в себя:

- угрозы внедрения вредоносного ПО;
- угрозы, реализуемые с использованием стандартных функций;
- угрозы, реализуемые в ходе загрузки операционной системы.

Результатом чего является нарушение конфиденциальности, целостности и доступности информации.

Основными причинами возникновения угроз для рассматриваемой организации могут являться:

- действия пользователей (преднамеренные или случайные);
- отсутствие или неэффективность технических средств защиты;
- отсутствие или недоработки организационных мер по ИБ.

В ИСПДн на базе автономного АРМ возможны все виды уязвимостей ИСПДн, за исключением уязвимостей, связанных с реализацией протоколов сетевого взаимодействия и каналов передачи данных. Уязвимостями, как было установлено ранее, являются:

- отсутствие организационно-распорядительных документов по ЗИ;
- незнание или игнорирование сотрудниками организационных требований;

- отсутствие необходимых средств защиты на АРМ.

Для устранения вышеуказанных причин в организации существуют некоторые меры обеспечения безопасности, такие как:

1) идентификация и аутентификация пользователей, являющихся сотрудниками организации;

Каждый из сотрудников должен иметь собственную учетную запись пользователя на АРМ, при помощи которой он сможет выполнять свои обязанности.

2) реализация правил разграничения доступа;

В соответствии с обязанностями сотрудника, присвоены права и привилегии доступа, обеспечен контроль за их соблюдением в соответствии с установленными в ИС правилами разграничения доступа.

3) антивирусная защита;

На АРМ, с помощью которых обрабатываются ПДн, должно быть установлено антивирусное программное обеспечение для обнаружения вредоносных программ в целях сохранения конфиденциальности, целостности и доступности информации.

4) регистрация событий безопасности;

В организации обеспечены меры по ведению журналов и отчетов о событиях безопасности, а также возможность просмотра и анализа информации о событиях безопасности.

5) анализ защищенности ПДн;

Проводятся мероприятия по тестированию работоспособности ИСПДн и анализу защищенности.

6)защита машинных носителей ПДн;

Специальные инструкции по безопасности обеспечивают защиту средств обработки и съемных носителей от несанкционированного доступа. Также, этому способствует система видеонаблюдения.

7)организационные меры по обеспечению ИБ.

К организационным мерам относятся организационно-распорядительные документы по защите и обработке информации, существующие в организации.

2.3. Угрозы, связанные с утечкой информации по техническим каналам

В ходе выявления актуальных угроз безопасности персональных данных в ИСПДн «Клиенты», угрозы, связанные с утечкой информации по техническим каналам, были приняты как неактуальные с маловероятной реализацией. Однако соблюдены меры и по предотвращению таких угроз, поэтому рассмотрим их и определим причины малой вероятности реализации.

К угрозам, связанным с утечкой информации по техническим каналам в ИСПДн относятся:

- утечка акустической информации;
- утечка видовой информации;
- утечка информации по каналам побочных электромагнитных излучений и наводок (ПЭМИН).

Источниками таких угроз могут являться физические лица или организации, использующие технические средства для их реализации.

Результатом действий также является нарушение конфиденциальности, целостности и доступности информации.

Рассмотрим каждую из угроз в отдельности:

1) угроза утечки акустической информации;

Под акустической информацией в ИСПДн принимается произносимая речь пользователя при обработке ПДн. Ввиду того, что в данной организации не используются акустические средства для воспроизведения ПДн и отсутствует функция голосового ввода – угроза является неактуальной.

2) утечка видовой информации;

Видовой информацией в организации является бумажная документация и архивные записи, а также информация, отображающаяся на экранах мониторов АРМ. Для обеспечения безопасности видовой информации в организации существуют организационно-распорядительные документы по работе с документацией, специальные сейфы для хранения и жалюзи на окнах для предотвращения возникновения прямой видимости.

3) утечка информации по каналам ПЭМИН.

Угроза перехвата информации возникает при обработке ПДн техническими средствами, когда образуются побочные электромагнитные излучения, которые могут распространяться за пределы защищаемого помещения. Так как активные средства защиты нецелесообразны к использованию в данной организации ввиду экономических затрат и минимальной вероятностью реализации подобной утечки – используются организационные меры. К ним относится проведение регулярных проверок и тестирований квалифицированным специалистом по защите информации, использование на объекте сертифицированных средств обработки и хранения ПДн, введение территориальных и временных ограничений в режимах использования технических средств, подлежащих защите.

2.4 Выбор средств защиты

В процессе анализа существующих угроз и уязвимостей было выявлено, что основными угрозами для безопасности ПДн организации являются угрозы несанкционированного доступа. Угроза утечки информации по техническим каналам не является актуальной, поэтому средства защиты от реализации данной угрозы рассматриваться не будут, так как в организации уже существует достаточное число организационных мер.

Для того чтобы выбрать подходящие средства защиты, рассмотрим их подробнее. Средствами защиты информации от несанкционированного доступа могут быть:

- электронные замки;
- электронные ключи и идентификаторы;
- автономные системы разграничения доступа;
- сетевые системы разграничения доступа;
- сертифицированные межсетевые экраны;

- средства построения VPN сетей;
- антивирусные средства.

Учитывая особенности ИСПДн организации, придем к выводу, что к использованию рациональным будет применить автономные системы разграничения доступа и антивирусные средства.

1) Автономные системы разграничения доступа.

Для обоснования выбора системы разграничения доступа составим таблицу основных наиболее существенных характеристик рассматриваемых систем. Полученная путем исследования информация представлена в таблице 7.

Таблица 7 – Характеристики систем разграничения доступа.

Характеристика	«Страж»	«Secret Net»	«Dallas Lock»
Поддержка ОС Microsoft	до Windows 10	до Windows 8.1	до Windows 10
Подсистема настройки системы защиты	+	+	+
Подсистема контроля целостности	+	+	+
Замкнутая программная среда	+	+	+
Подсистема мандатного разграничения доступа	+	+	-
Подсистема регистрации событий	+	+	+
Стоимость, руб.	15000	9185	10200

Проанализировав таблицу, можно заметить, что все их представленных систем имеют функционал, полностью соответствующий потребностям ИСПДн организации. Это означает, что выбор средства будет основан на его экономической составляющей, где фаворитом является СЗИ «Secret Net». Кроме того, важным условием выбора было то, что сотрудник уже имел опыт работы с данным СЗИ. Поэтому в качестве автономного средства разграничения доступа рекомендуется ввести в пользование СЗИ «Secret Net». Актуальной версией продукта является версия 7.6.

2) Антивирусное программное обеспечение.

Выбор антивирусного средства для организации непосредственно зависит от ее размеров. Так как мы рассматриваем ПО для небольшой организации, то эффективным будет использование не отдельного продукта для решения конкретной задачи, а комплексного решения. Таким образом, в пакет предоставляемых услуг

помимо антивируса может входить брандмауэр, контроль устройств, антиспам, элемент управления мобильными устройствами и другое.

Важным условием выбора является то, что для защиты персональных данных необходимо использовать средства антивирусной защиты, прошедшие процедуру оценки соответствия. В соответствии с Государственным реестром сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 в настоящее время действующий сертификаты имеют программные средства, такие как:

- антивирус Dr.Web Enterprise Security Suite версии 10;
- антивирус Kaspersky Endpoint Security версии 10 для Windows Workstations.

Так как данные средства имеют схожий функционал, выбор средства может быть основан на экономической составляющей. Стоимость продуктов, установленная производителем, представлена в таблице 8.

Таблица 8 – Стоимость антивирусных средств.

Название	Стоимость, руб.
Dr.Web Enterprise Security Suite версии 10	5990
Kaspersky Endpoint Security версии 10	5850

Как видно, разница в цене является несущественной, поэтому выбор средства может зависеть от иных факторов, учитывая личные предпочтения. Но для данного проекта, обосновав свой выбор экономической целесообразностью, в качестве антивирусного программного обеспечения рекомендуется использовать Kaspersky Kaspersky Endpoint Security версии 10.

ВЫВОДЫ ПО ВТОРОЙ ГЛАВЕ

Вторая глава работы была посвящена проведению обзора на возможные методы устранения уязвимости, общему описанию угроз безопасности ИСПДн и выбору средств защиты.

В ходе работы, в соответствии с разработанной ранее моделью угроз и уязвимостей, подробным образом были описаны угрозы безопасности связанные с НСД и утечкой информации по техническим каналам. Остальные угрозы безопасности ИСПДн, на основе «Базовой модели угроз безопасности информации при их обработке в ИСПДн» ФСТЭК России от 15 февраля 2008 г. были признаны неактуальными и не рассмотрены в рамках данной работы.

Выбор методов по обеспечению безопасности персональных данных, подлежащих реализации в ИС в рамках системы защиты персональных данных основан на Приказе ФСТЭК от 18 февраля 2013 года №21 «Об утверждении Состава и содержании организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Для выбора средств защиты от НСД были произведены сравнения характеристик различных программных средств, в результате которых были выявлены рекомендуемые средства – СЗИ «Secret Net 7.6.» и антивирусное ПО «Kaspersky Endpoint Security 10». В качестве защиты от угроз утечки информации по техническим каналам, ввиду малой вероятности реализации таких утечек, средства защиты не предусмотрены.

ГЛАВА 3 РАЗРАБОТКА ПРОЕКТА СИСТЕМЫ ЗАЩИТЫ В ООО МФО «ГОРОДСКОЙ ЗАЙМ»

3.1. Описание объекта

Основным видом деятельности ООО МФО «Городской Займ» является предоставление потребительских кредитов населению. Организация в числе первых начала функционировать на рынке восточного Оренбуржья. Общество создано в 2011 году, зарегистрировано в реестре микрофинансовых организаций в Федеральной службе по финансовым рынкам.

Основной информацией, циркулирующей в организации, являются персональные данные физических лиц и сотрудников.

Подробная структура защищаемой информации представлена в таблице 9.

Таблица 9 – Защищаемая информация.

Входящая	Исходящая
Документооборот в пределах организации	
ПДн клиентов	База данных клиентов
	Сведения о предоставленных кредитах
	Отчетность

3.2 Резюме проекта

В ходе разработки проекта необходимо определить ряд организационно-технических и программно-аппаратных мер. Организационно-технические меры наглядно отображены в матрице ответственности, где за каждым этапом разработки проекта закреплены ответственные лица и определены объекты поставки.

Разработка проекта была произведена в соответствии с утвержденным техническим заданием на создание системы защиты ИСПДн ООО МФО «Городской Займ».

Техническое задание представлено в Приложении Г.

Результатом разработки проекта является автоматизированная система обработки персональных данных, обеспечивающая систему защиты ИСПДн от НСД и соответствующая требованиям нормативно-правовой документации.

3.3Цели и задачи проекта

Для разработки проекта системы защиты ООО МФО «Городской Займ» были поставлены следующие цели:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копирования, блокированию информации;

- предотвращение других форм незаконного вмешательства в информационные ресурсы и системы, обеспечение правового режима информации как объекта собственности;

- защита персональных данных в соответствии с требованиями действующих руководящих документов ФСБ России и ФСТЭК России.

Задачами проекта являются:

- развитие системы информационной безопасности в направлениях обеспечения организационно-технической и программно-аппаратной безопасности;

- анализ процессов управления информационной безопасностью;

- реализация мероприятий по защите персональных данных.

3.4. Объекты поставки проекта

1) Организационно-распорядительная документация:

- политика в отношении обработки персональных данных;

- должностные инструкции сотрудников.

2) Программно-аппаратные и инженерно-технические меры:

- средство защиты от НСД(Secret Net 7.6.);

- антивирусное ПО(Kaspersky Endpoint Security 10).

3) Обучение персонала.

В рамках реализации проекта необходимо провести обучение сотрудников организации новым требованиям защиты информации с обоснованием необходимости и значимости их квалифицированности. Данное мероприятие обусловлено внедрением новых организационно-распорядительных документов и программно-аппаратных мер, предусмотренных проектом.

3.5 Риски проекта

Для расчета рисков проекта введем следующие обозначения:

P(V) - вероятность реализации угрозы через данную уязвимость в течение года;

ER - критичность реализации угрозы через уязвимость;

Th - уровень угрозы;

CTh - уровень угрозы по всем уязвимостям, через которые реализуется данная угроза.

Для расчета уровня угрозы воспользуемся формулой:

$$Th = \frac{ER}{100} \times \frac{P(V)}{100}$$

Уровень угрозы по всем уязвимостям, через которые реализуется данная угроза CTh, рассчитывается по формуле:

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

Оценка рисков произведена на основании данных открытых источников. Показатели рисков проекта представлены в таблице 10.

Таблица 10 – Риски проекта.

Риски и пути их реализации	ER, (%)	P(V), (%)	Th, (%)	CTh, (%)
1	2	3	4	5
Риски изменений в стране, обществе				
Ухудшение политических и экономических характеристик				0,017
Реформы в политике и экономике	15	5	0,007	
Изменение законодательства	20	5	0,01	
Изменение факторов общества				0,320
Возникновение негативного отношения сотрудников	80	40	0,32	
Влияние форс-мажорных обстоятельств				0,015
Стихийные бедствия и природные катаклизмы	30	5	0,015	
Риски окружения проекта в составе организации				
Изменение или недостаток бюджета проекта				0,827
Задержки финансирования	90	10	0,09	
Отсутствие денежного резерва для реагирования на события рисков	90	90	0,81	
Недостаточная организованность работ				0,040
Срыв графиков работ, невыполнение сроков	20	10	0,02	
Нехватка рабочей силы	30	5	0,015	
Недооценка стоимости работ и использование финансов для других целей	30	2	0,006	
Риски персонала				0,044
Влияние личностных факторов	25	10	0,025	
Риск недоступности персонала, которому сложно подобрать замену	20	10	0,02	

Получив в результате расчетов уровень угроз по всем уязвимостям, можно представить насколько критичным является воздействие конкретной угрозы на ресурс с учетом вероятности ее реализации.

Максимальным уровнем угрозы обладает риск изменения или недостатка бюджета – 0,827. Он включает в себя как риск задержки финансирования, так и отсутствие денежного резерва для реагирования на события рисков. Минимальный уровень угрозы – 0,015, соответствует риску влияния стихийных бедствий и природных катастроф.

3.6. Структура разбиения работ

Структура разбиения позволит определить единую структуру управления проектом. Она является эффективным инструментом для четкого определения работ и сопоставления плана проекта с потребностями заказчика, необходимых для реализации проекта.

1) Содержание структуры разбиения работ по разработке ИСПДн представлено в таблице 11.

Таблица 11 - Структура разбиения работ.

Обозначение этапа	Наименование этапа работы
ИСПДн 1.	Проектирование
ИСПДн 1.1.	Определение текущих бизнес-процессов
ИСПДн 1.2.	Анализ проблем текущих бизнес-процессов
ИСПДн 1.3.	Разработка значений ключевых показателей новых бизнес-процессов
ИСПДн 1.4.	Анализ и выбор методов и способов улучшения значений показателей бизнес-процессов
ИСПДн 1.5.	Разработка и согласование структуры новых бизнес-процессов
ИСПДн 2.	Совершенствование организационно распорядительной документации
ИСПДн 2.1.	Политика в отношении обработки ПДн
ИСПДн 2.2.	Внесение изменений в должностные инструкции сотрудников
ИСПДн 2.3.	Согласование и утверждение документации
ИСПДн 3.	Подготовка реализации проекта
ИСПДн 3.1.	Определение ответственных лиц и исполнителей проекта
ИСПДн 3.2.	Приобретение антивирусного ПО
ИСПДн 3.3.	Приобретение средства защиты от НСД
ИСПДн 4.	Внедрение
ИСПДн 4.1.	Установка и настройка антивирусного ПО
ИСПДн 4.2.	Установка и настройка средств защиты от НСД
ИСПДн 4.3.	Контроль защищенности
ИСПДн 4.4	Обучение пользователей

Наглядное изображение структуры разбиения представлено на рисунке 1.

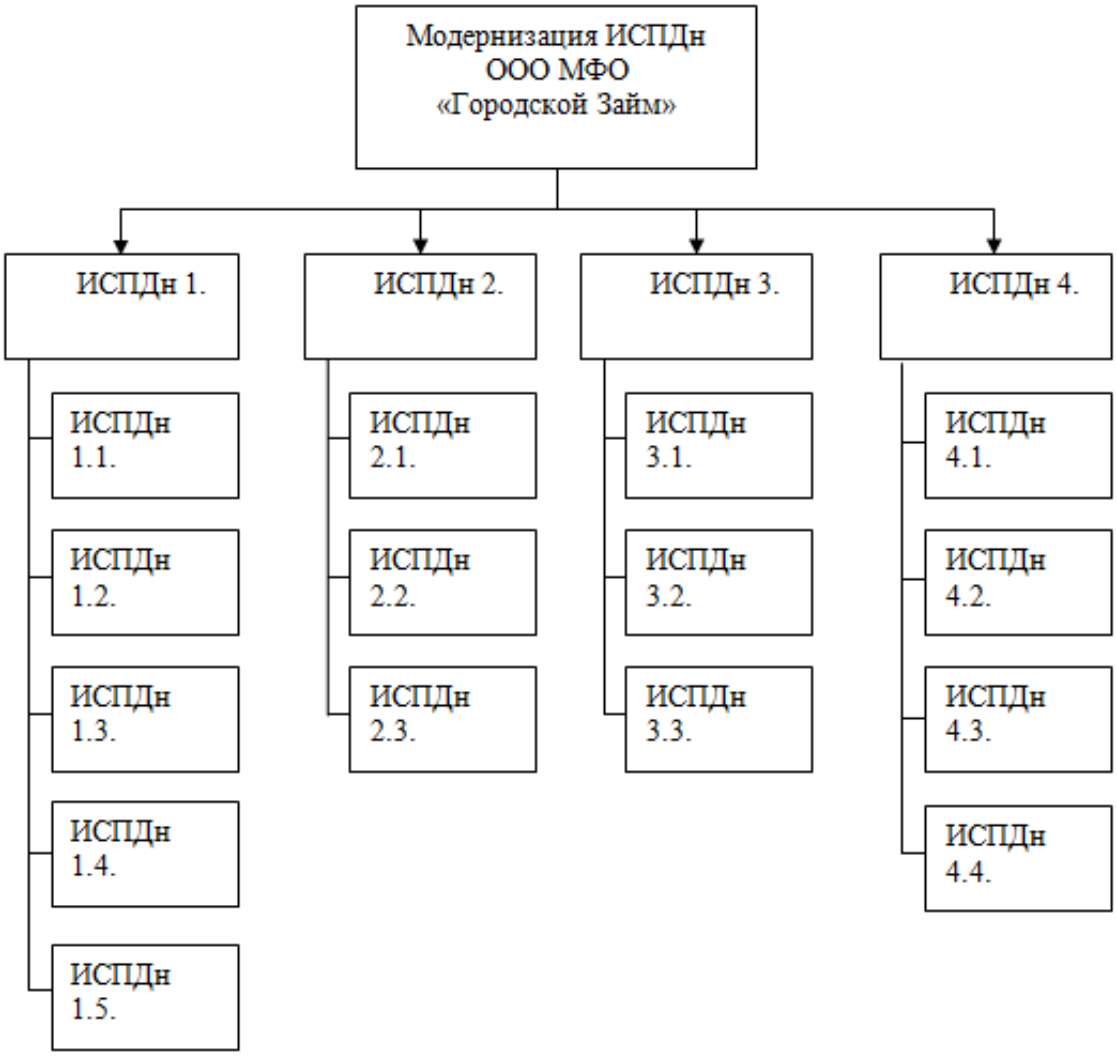

Рис.1 - Структура разбиения работ

3.7. Структурная схема организации проекта

Структурная схема организации проекта необходима для распределения ролей и обязанностей среди сотрудников, задействованных в процессе реализации проекта.

Перечень сотрудников:

1. Менеджер проекта;
2. Директор;
2.1. Бухгалтерия;
3. Начальник ИТ отдела;
3.1. Специалист по ЗИ.

Данная схема представлена на рисунке 2.

Рис.2 - Структурная схема организации проекта

3.8. Матрица ответственности

Матрица ответственности позволит установить степень ответственности каждого из сотрудников организации, участвующих в проекте. Для каждого из возможных действий установим обозначения:

- К - контроль;
- У - управление;
- И - исполнение.

В соответствии со структурой разбиения работ и структурной схемой организации проекта составим матрицу. Матрица ответственности представлена в таблице 12.

Таблица 12 - Матрица ответственности.

Обозначение этапа	Участники проекта				
	1.	2.	2.1.	3.	3.1
1	2	3	4	5	6
ИСПДн 1.	К				
ИСПДн 1.1.	К/У				И
ИСПДн 1.2.	И				К
ИСПДн 1.3.	И				К
ИСПДн 1.4.	К/У				К
ИСПДн 1.5.	И				У/И
ИСПДн 2.	К				У/И
ИСПДн 2.1.	К				У/И
ИСПДн 2.2.	К				У/И
ИСПДн 2.3.	К				У/И
ИСПДн 3.	К				

Продолжение таблицы 11.

1	2	3	4	5	6
ИСПДн 3.1.	К				И
ИСПДн 3.2.	К				
ИСПДн 3.3.	К				
ИСПДн 4.	К				И
ИСПДн 4.1.	К				И
ИСПДн 4.2.	К				И
ИСПДн 4.3.	К				И
ИСПДн 4.4	И		К		К

3.9. Диаграмма Ганта и сетевой график

Для наглядного представления графика работ по проекту необходимо составить диаграмму Ганта. Важной частью диаграммы является отображение зависимости одной задачи от другой. Для начала нужно определить период, в течение которого должна быть выполнена задача.

Распределение сроков выполнения работ представлено в таблице 13.

Таблица 13 – Распределение сроков.

Обозначение этапа	Наименование этапа работы	Длительность	Начало	Окончание
1	2	3	4	5
ИСПДн 1.	Проектирование	13	1.09.2017	13.09.2017
ИСПДн 1.1.	Определение текущих бизнес-процессов	3	1.09.2017	3.09.2017
ИСПДн 1.2.	Анализ проблем текущих бизнес-процессов	2	4.09.2017	5.09.2017
ИСПДн 1.3.	Разработка значений ключевых показателей новых бизнес-процессов	3	6.09.2017	8.09.2017
ИСПДн 1.4.	Анализ и выбор методов и способов улучшения значений показателей бизнес-процессов	2	9.09.2017	10.09.2017
ИСПДн 1.5.	Разработка и согласование структуры новых бизнес-процессов	3	11.09.2017	13.09.2017
ИСПДн 2.	Совершенствование организационно распорядительной документации	7	13.09.2017	20.09.2017
ИСПДн 2.1.	Политика в отношении обработки ПДн	3	13.09.2017	15.09.2017

Продолжение таблицы 12.

1	2	3	4	5
ИСПДн 2.2.	Внесение изменений в должностные инструкции сотрудников	2	16.09.2017	17.09.2017
ИСПДн 2.3.	Согласование и утверждение документации	2	18.09.2017	19.09.2017
ИСПДн 3.	Подготовка реализации проекта	2	20.09.2017	21.09.2017
ИСПДн 3.1.	Определение ответственных лиц и исполнителей проекта	1	20.09.2017	20.09.2017
ИСПДн 3.2.	Приобретение антивирусного ПО	1	21.09.2017	21.09.2017
ИСПДн 3.3.	Приобретение средства защиты от НСД	1	21.09.2017	21.09.2017
ИСПДн 4.	Внедрение	2	22.09.2017	23.09.2017
ИСПДн 4.1.	Установка и настройка антивирусного ПО	1	22.09.2017	22.09.2017
ИСПДн 4.2.	Установка и настройка средств защиты от НСД	1	22.09.2017	22.09.2017
ИСПДн 4.3.	Контроль защищенности	1	23.09.2017	23.09.2017
ИСПДн 4.4	Обучение пользователей	1	23.09.2017	23.09.2017

Используя данные составленной таблицы, построим диаграмму Ганта. Диаграмма представлена на рисунке 3.

В соответствии с данной таблицей и диаграммой Ганта срок выполнения проекта составляет 22 дня.

Сетевой график предназначен для отображения зависимостей между всеми работами по осуществлению проекта, а также наглядного представления определенной последовательности выполнения задач.

Построение сетевого графика мы начнем на основе выполненной диаграммы Ганта. Для этого определим сроки выполнения работ, представив их в таблице 14.

Примем следующие обозначения:

- i-j – код работы;
- Т – длительность работы в днях;
- Трн – ранний срок начала работы;
- Тпн – поздний срок начала работы;
- Тро – ранний срок окончания работы;
- Тпо – поздний срок окончания работы.

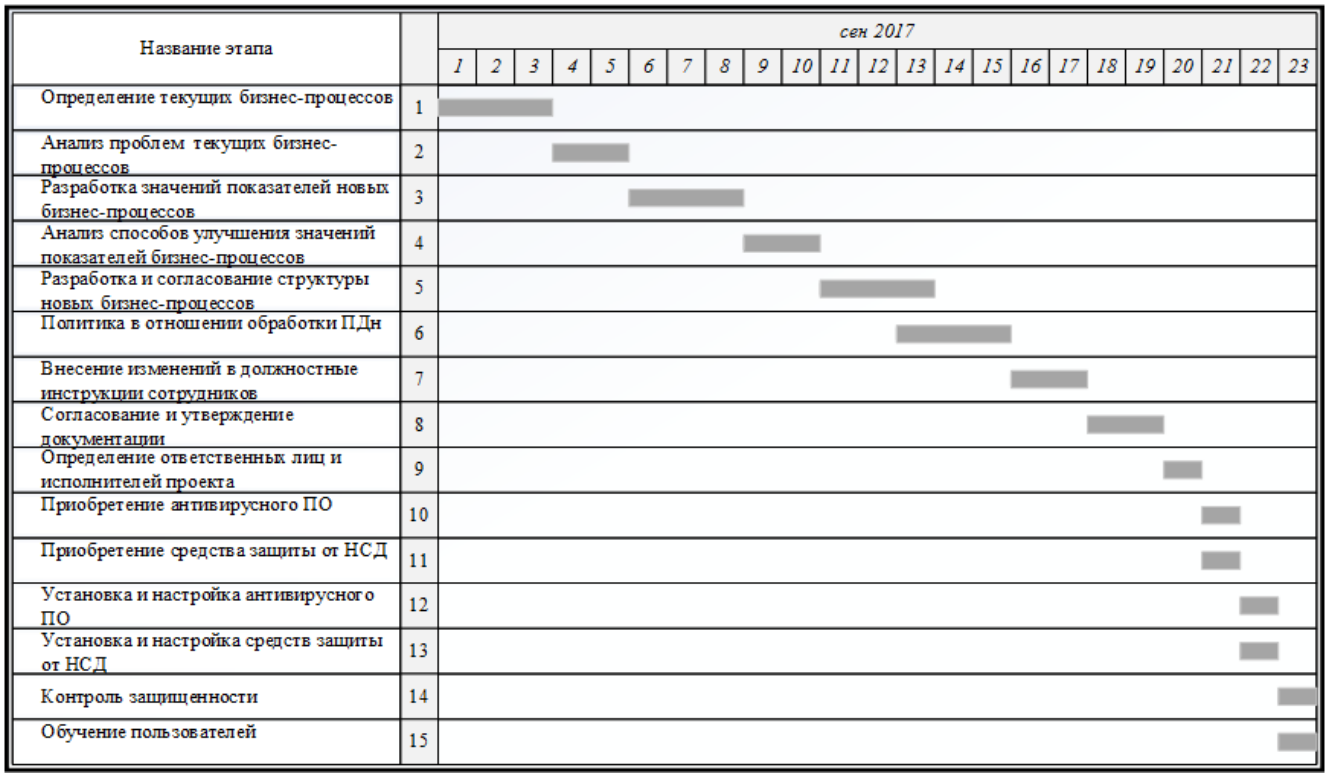

Рис. 3 - Диаграмма Ганта

Таблица 14 - Сроки выполнения работ.

Обозначение этапа	Наименование этапа работы	Код	Т	$T_{рн}$	$T_{пн}$	$T_{ро}$	$T_{по}$
1	2	3	4	5	6	7	8
ИСПДн 1.	Проектирование		13	0	0	13	13
ИСПДн 1.1.	Определение текущих бизнес-процессов	1-2	3	0	0	3	3
ИСПДн 1.2.	Анализ проблем текущих бизнес-процессов	2-3	2	3	3	5	5
ИСПДн 1.3.	Разработка значений ключевых показателей новых бизнес-процессов	3-4	3	5	5	8	8
ИСПДн 1.4.	Анализ и выбор методов и способов улучшения значений показателей бизнес-процессов	4-5	2	8	8	10	10
ИСПДн 1.5.	Разработка и согласование структуры новых бизнес-процессов	5-6	3	10	10	13	13

Продолжение таблицы 13.

1	2	3	4	5	6	7	8
ИСПДн 2.	Совершенствование организационно распорядительной документации		7	13	13	20	20
ИСПДн 2.1.	Политика в отношении обработки ПДн	6-7	3	13	13	16	16
ИСПДн 2.2.	Внесение изменений в должностные инструкции сотрудников	7-8	3	16	16	19	19
ИСПДн 2.3.	Согласование и утверждение документации	8-9	2	19	19	21	21
ИСПДн 3.	Подготовка реализации проекта		2	21	21	23	23
ИСПДн 3.1.	Определение ответственных лиц и исполнителей проекта	9-10	1	21	21	22	22
ИСПДн 3.2.	Приобретение антивирусного ПО	10-11	1	22	22	23	23
ИСПДн 3.3.	Приобретение средства защиты от НСД	11-12	1	22	22	23	23
ИСПДн 4.	Внедрение		2	23	23	25	25
ИСПДн 4.1.	Установка и настройка антивирусного ПО	12-13	1	23	23	24	24
ИСПДн 4.2.	Установка и настройка средств защиты от НСД	13-14	1	23	23	24	24
ИСПДн 4.3.	Контроль защищенности	14-15	1	24	24	25	25
ИСПДн 4.4	Обучение пользователей	15-16	1	24	24	25	25

ВЫВОД ПО ТРЕТЬЕЙ ГЛАВЕ

Третья глава была посвящена разработке проекта системы защиты ИСПДн «Клиенты» ООО МФО «Городской Займ». Процесс разработки состоял из последовательного выполнения ряда иерархически структурированных работ, необходимых для реализации проекта.

В ходе выполнения работ было составлено описание объекта, содержащее данные об основном виде деятельности ООО МФО «Городской Займ» и защищаемой информации. Для разработки проекта было составлено резюме проекта, представляющее собой краткое описание необходимых работ, также определены объекты поставки, цели и задачи проекта. На основании данных открытых источников была произведена оценка и расчет рисков проекта, в результате которых был выявлена наиболее критичная угроза – изменение или недостаток бюджета. Составлена структура разбиения работ, структурная схема организации проекта, перечень ответственных лиц. В соответствии со структурой разбиения работ и структурной схемой организации проекта была составлена матрица ответственности, сетевой график и диаграмма Ганта, на основании которых был установлен срок реализации проекта – 22 дня.

В результате реализации разработанного проекта уровень обеспечения информационной безопасности персональных данных в организации значительно увеличится, поэтому внедрение данного проекта в организацию является необходимым мероприятием по усовершенствованию защиты информации и соблюдению требований законодательства.

ЗАКЛЮЧЕНИЕ

Результатом выполнения выпускной квалификационной работы является произведенный анализ состояния защиты информации в ООО МФО «Городской Займ». Для формирования общего представления об объекте ВКР был составлен паспорт организации с точки зрения информационной безопасности и выбран защищаемый объект. В результате анализа разработанной модели деятельности объекта была выявлена информация ограниченного доступа и выявлены объекты защиты. На основании документов ФСТЭК для объектов защиты была разработана модель угроз и уязвимостей, определен уровень исходной защищенности информационной системы.

На основании полученных в результате анализа данных, в ходе выполнения выпускной квалификационной работы было разработано техническое задание на создание системы защиты ИСПДн. Перед тем, как начать разработку проекта, было проведено теоретическое обоснование выбора средств защиты, в ходе которого, кроме непосредственного анализа средств защиты информации, были подробно описаны существующие угрозы.

Завершающим этапом проведения предпроектного исследования стала разработка проекта системы защиты информации в ООО МФО «Городской Займ». Процесс разработки включает в себя составление резюме проекта, определение целей и задач, расчет рисков и составление структуры разбиения работ. Структурная схема организации проекта и матрица ответственности эффективно распределить ответственность среди участников организации, задействованных в процессе реализации проекта. Для наглядного представления графика работ, сроков и последовательности их выполнения

Разработанный проект позволит усовершенствовать систему защиты персональных данных в организации, снизить возможные риски угроз безопасности и повысить общий уровень информационной безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: (выписка): утв. ФСТЭК России от 15.02.2008 г.// ФСТЭК России [Электронный ресурс], - Техническая защита информации. - М, 2017.

2. ГОСТ 34.201-89.Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем. - Введ. 01.01.1990. - М.:Издательство стандартов, 1989. - 11 с.

3. ГОСТ Р 50922-2006.Защита информации. Основные термины и определения. – Введ. 01.02.2008. – М.: Госстандарт России, 2001.– 12 с.

4. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: утв. ФСТЭК России от 14.02.2008 г.// ФСТЭК России [Электронный ресурс], - Техническая защита информации. - М, 2017.

5. «О персональных данных»: федеральный закон Российской Федерации от 27.07.2006 № 152 - ФЗ:(в ред. от 22.02.2017): принят Гос. Думой 8 июля 2006 г.: одобрен Советом федерации 14 июля 2006 г. // КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2017.

6. «Об информации, информационных технологиях и защите информации»: федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ: (ред. от 19.12.2016): принят Гос. Думой 8 июля 2006 г.: одобрен Советом федерации 14 июля 2006 г.// КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

7. Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: приказ ФСТЭК России от 18.02.2013 №21// ФСТЭК России [Электронный ресурс], - Техническая защита информации. - М, 2017.

8. «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: постановление правительства Российской Федерации от 1 ноября 2012 г. N 1119// КонсультантПлюс. Технология 3000: Интернет-версия [Электронный ресурс] / ЗАО «КонсультантПлюс». – Электрон. дан. и прогр. – М., 2015.

ПРИЛОЖЕНИЕ А

Общество
с ограниченной ответственностью
микрофинансовая организация
«ГОРОДСКОЙ ЗАЙМ»

ИНН 5607043734, КПП 560701001, ОГРН 11156580009114, ОКПО 90485194
462371, Оренбургская область, г. Новотроицк, пгт. Аккермановка, ул. Восточная, 1А
Телефон: 66-05-11, 8-903-3699016

ПАСПОРТ ПРЕДПРИЯТИЯ

С точки зрения обеспечения
информационной безопасности

УТВЕРЖДАЮ
Директор
ООО МФО «Городской Займ»
_____С.Т.Искулов
Дата_____

Паспорт предприятия ООО МФО «Городской Займ»

Содержание паспорта предприятия:

1.1.1. Организационно-правовая форма организации и ее реквизиты

1. Название организации:
   Общество с ограниченной ответственностью микрофинансовая организация «Городской Займ».
2. Численность сотрудников:
   18 человек.
3. Банковские реквизиты:
   ИНН 5607043734
   КПП 560701001
   ОГРН 11156580009114
   ОКПО 90485194

1.1.2. Вид деятельности предприятия

Предоставление потребительского кредита.

1.1.3. Наличие лицензий

Свидетельство о внесении сведений об организации в государственный реестр микрофинансовых организаций.

1.1.4. Предполагаемые виды защищаемой информации

Персональные данные.

1.1.5. Перечень клиентов:

Клиентами ООО МФО «Городской Займ» являются физические лица.

1.1.6. Описание организационной структуры предприятия

Организационная структура ООО МФО «Городской Займ» включает в себя:

1. Директор
1.2. Заместитель директора
1.3. Главный бухгалтер
1.3.1. Бухгалтерия
1.4. Операторы- консультанты

1.1.7. Описание информационной среды организации

В информационную среду организации входят базы данных сотрудников и клиентов.

Программно-аппаратные средства:

1. Операционная система семейства Windows.
2. Пакет программ Microsoft Office
2.1. Microsoft Word - используется для оформления договоров и отчетности.
2.2. Microsoft Excel – используется для работы с отчетностью и базами данных.
2.3. Microsoft Access – используется для управления базами данных.
2.4. Microsoft Visio – используется для создания схем, организационных диаграмм, блок-схем, планов и визуализации информации.
3. Microsoft Security Essentials – используется в качестве антивирусного программного обеспечения.
4. Кредитный инспектор - используется для автоматизации процесса оформления займов.
5. Internet Explorer – используется для просмотра разных типов веб-страниц и установки обновлений.
6. 7-Zip - архиватор для сжатия данных.
7. Foxit Reader – используется для просмотра электронных документов.

1.1.8. Описание строительной инфраструктуры зданий и сооружений, описание местоположения организации

Офис организации располагается в здании по адресу ул. Зеленая 33. Здание располагается около проезжей части, окружено жилыми домами.

1. Пятиэтажное жилое здание, не имеет дополнительных ограждений.
2. Установлена система автоматической пожарной сигнализации, система видеонаблюдения и адресная охранно-пожарная система.
3. Функционирует система центрального водяного отопления.
4. Имеется пожарный щит с пожарным рукавом и огнетушителем.
5. Общая телефонная сеть.

1.1.9. Сведения о защищаемом помещении

Сведения об отделе по работе с клиентами:

1. Название:
Отдел по работе с клиентами

2. Местоположение:
ул. Зеленая 33, первый этаж, помещение №2.
3. Количество сотрудников отдела: 1
4. Организационная структура отдела:
1. Оператор-консультант
5. Информационная среда отдела представлена в таблице 1.

Таблица 1 – Информационная среда отдела

Программа	Назначение
Пакет программ Microsoft Office	Работа с отчетностью, договорами и базами данных
Microsoft Security Essentials	Антивирусное программное обеспечение
Кредитный инспектор	Автоматизация процесса оформления займов

6. План этажа и схема помещения:

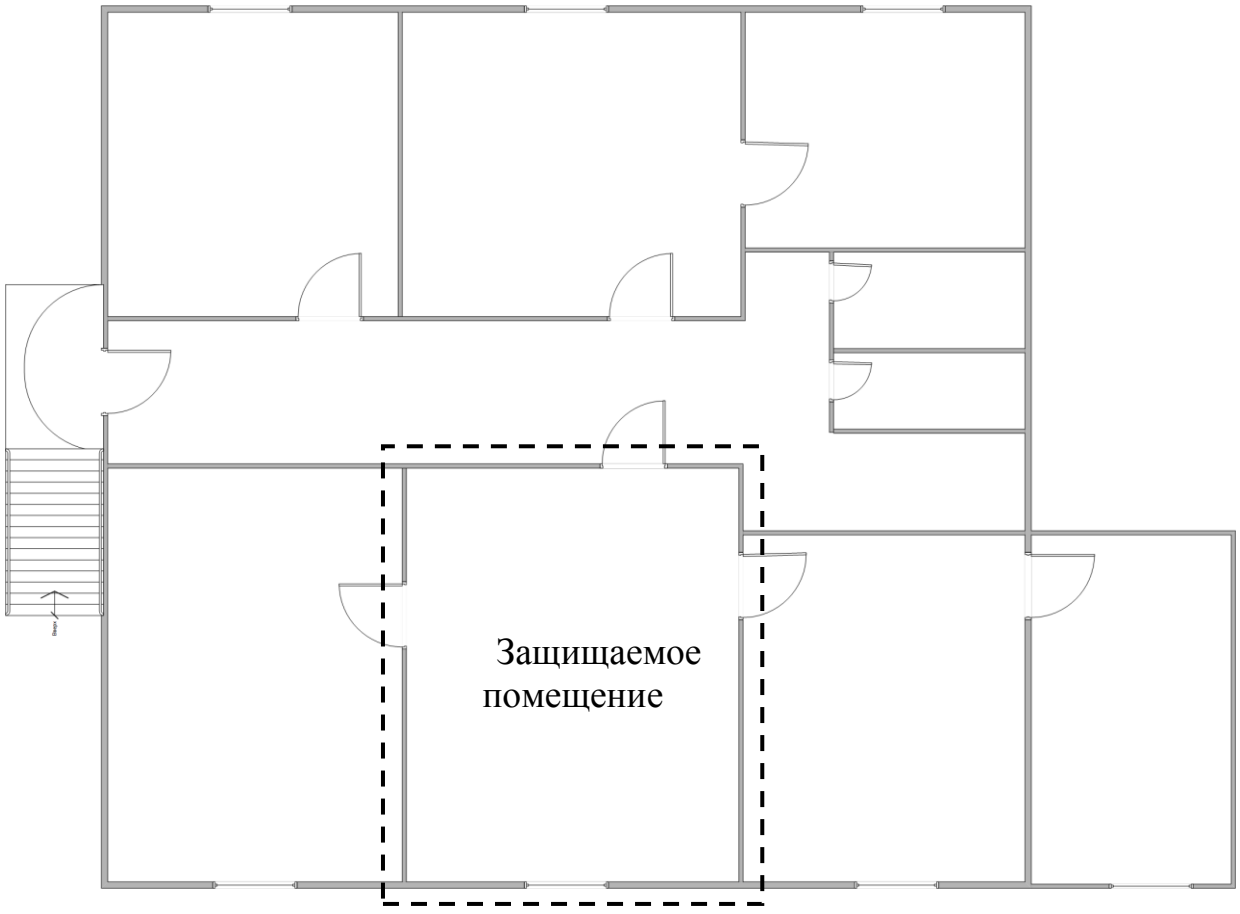

Рис.1 – План этажа

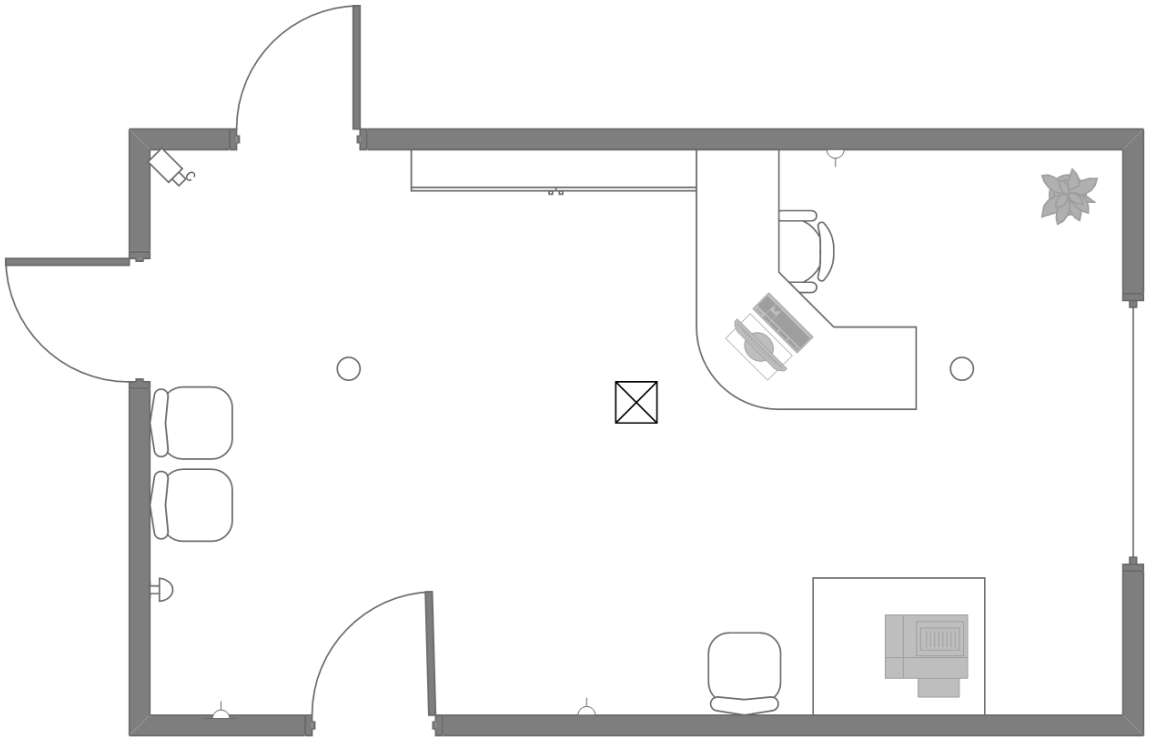

Рис.2 – Схема помещения

ПРИЛОЖЕНИЕ Б

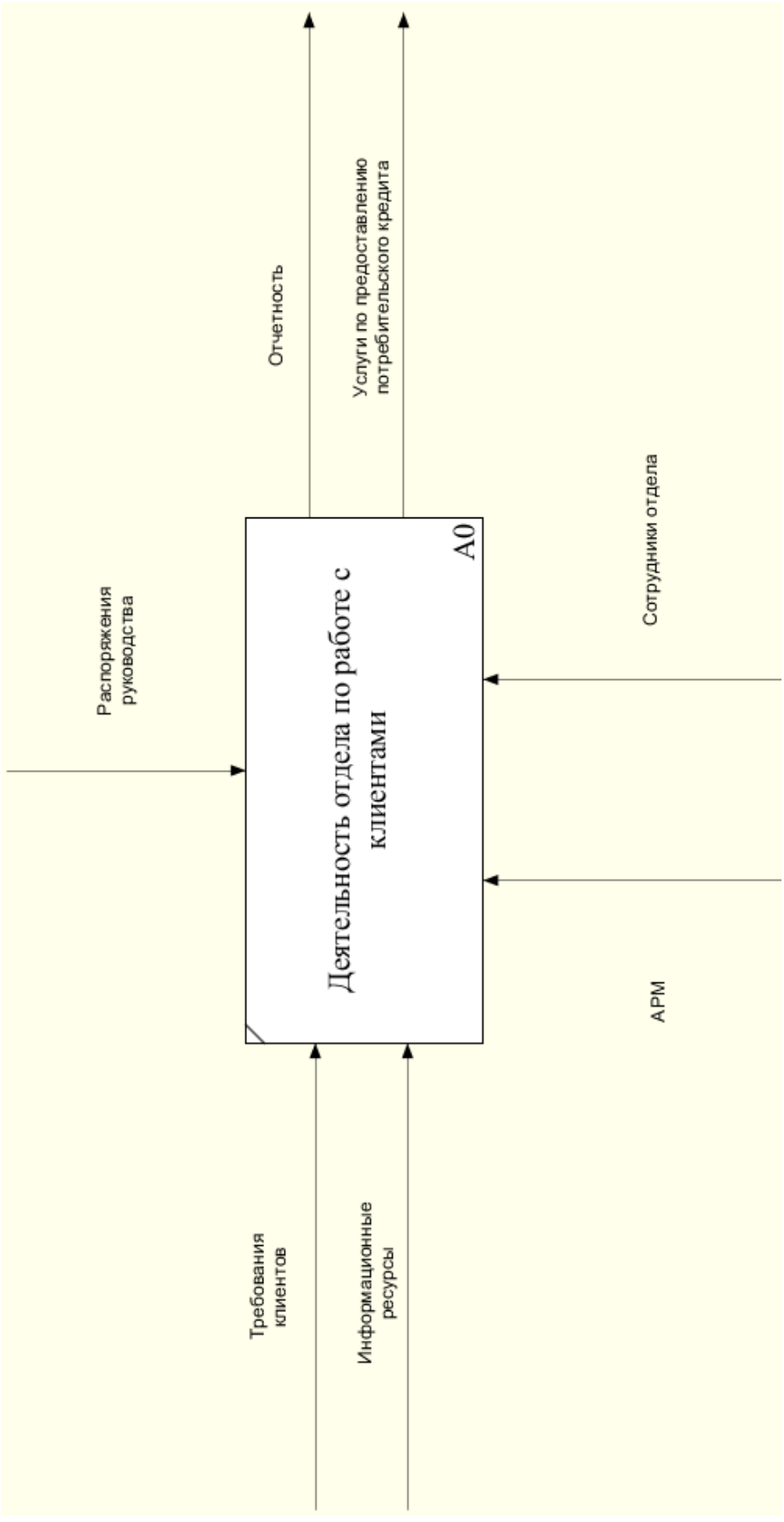

Рис.1 – Модель деятельность отдела по работе с клиентами

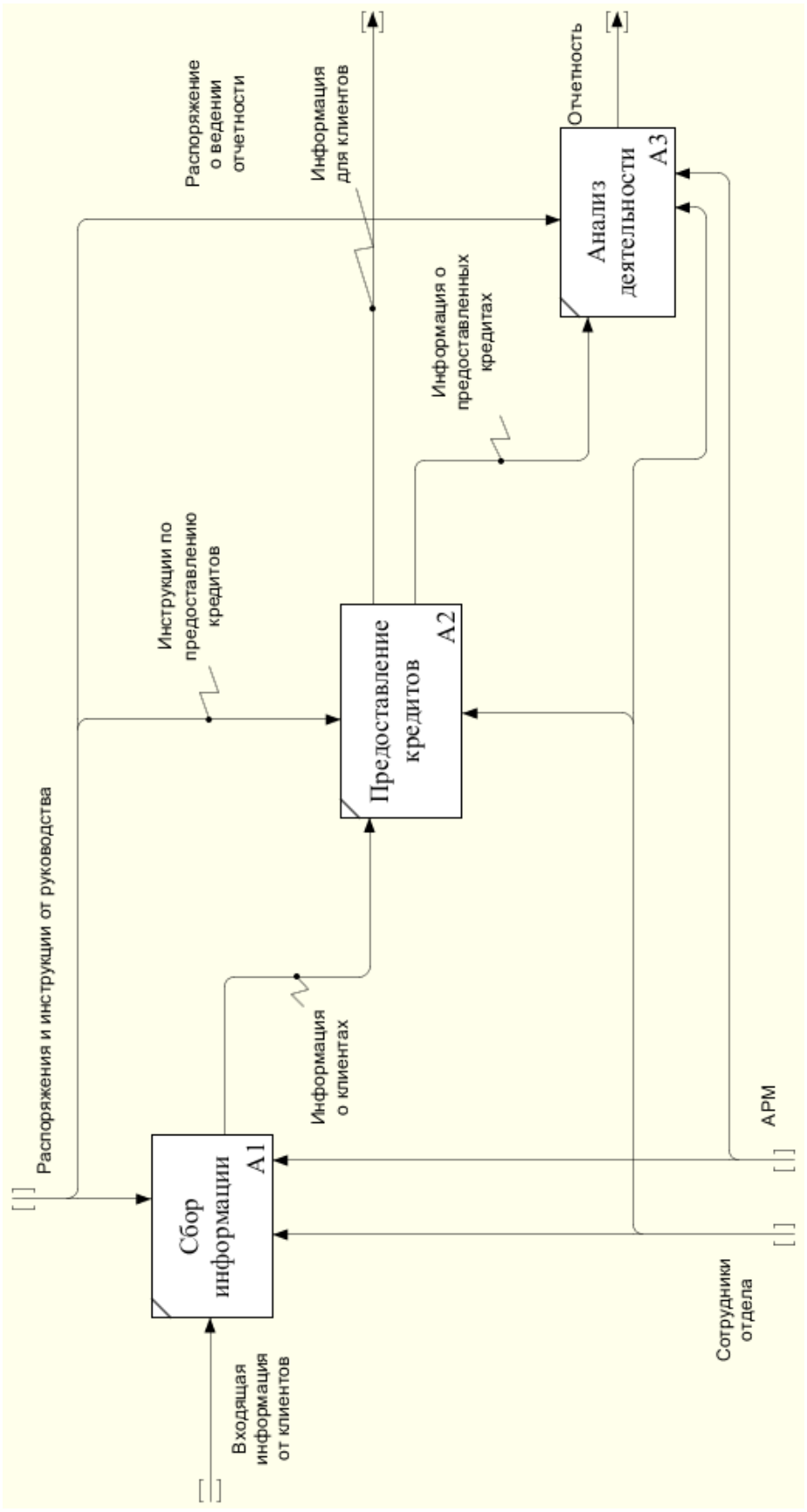

Рис.2 – Модель описания деятельности отдела по работе с клиентами

ПРИЛОЖЕНИЕ В

Общество
с ограниченной ответственностью
микрофинансовая организация
«ГОРОДСКОЙ ЗАЙМ»

ИНН 5607043734, КПП 560701001, ОГРН 11156580009114, ОКПО 90485194
462371, Оренбургская область, г. Новотроицк, пгт. Аккермановка, ул. Восточная, 1А
Телефон: 66-05-11, 8-903-3699016

ПОЛИТИКА
в отношении обработки
персональных данных

УТВЕРЖДАЮ
Директор
ООО МФО «Городской Займ»
_____С.Т.Искулов
Дата_____

Политика в отношении обработки персональных данных

1. ВВЕДЕНИЕ

1.1 Важнейшим условием реализации целей деятельности ООО МФО «ГОРОДСКОЙ ЗАЙМ» (далее - Общество), является обеспечение необходимого и достаточного уровня информационной безопасности активов, к которым в том числе относятся персональные данные

1.2 Обеспечение безопасности персональных данных является одной из приоритетных задач Общества.

1.3 Обработка и обеспечение безопасности информации, отнесенной к персональным данным в Обществе осуществляется в соответствии с Комплексом документов Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» и позволяет обеспечить защиту персональных данных, обрабатываемых как в информационных системах персональных данных, т.е. в системах, целью создания которых является обработка персональных данных и к защите которых требования и рекомендации по обеспечению безопасности персональных данных предъявляют Федеральная служба безопасности Российской Федерации (ФСБ России), Федеральная служба по техническому и экспортному контролю (ФСТЭК России), так и в иных информационных системах, в которых персональные данные обрабатываются совместно с информацией, защищаемой в соответствии с требованиями, установленными для этой информации (режим защиты сведений, составляющих банковскую тайну, коммерческую тайну и др.).

1.4 Настоящая Политика определяет принципы, порядок и условия обработки персональных данных работников Общества и иных лиц, чьи персональные данные обрабатываются Обществом, с целью обеспечения защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну, а так-

же устанавливает ответственность должностных лиц Общества, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных.

1.6 Персональные данные являются конфиденциальной, строго охраняемой информацией и на них распространяются все требования, установленные внутренними документами Общества к защите конфиденциальной информации.

2. ПОНЯТИЕ И СОСТАВ ПЕРСОНАЛЬНЫХ ДАННЫХ

2.1 Перечень персональных данных, подлежащих защите в Обществе, формируется в соответствии с ФЗ РФ от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и Уставом Общества.

2.2 Сведениями, составляющими персональные данные, в Обществе является любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

2.3 В зависимости от субъекта персональных данных, Общество обрабатывает персональные данные следующих категорий субъектов персональных данных:

- персональные данные работника Общества — информация, необходимая Общества в связи с трудовыми отношениями и касающиеся конкретного работника.

- персональные данные аффилированного лица или персональные данные руководителя, участника или сотрудника юридического лица, являющегося аффилированным лицом по отношению к Обществу — информация, необходимая Обществу для отражения в отчетных документах о деятельности Общества в соответствии с требованиями федеральных законов, нормативных документов Банка России и иных нормативных правовых актов.

- персональные данные Клиента, а также персональные данные руководителя, участника или сотрудника юридического лица, являющегося Клиентом Общества - информация, необходимая Обществу для выполнения своих обязательств в рамках договорных отношений с Клиентом и для выполнения требований законодательства Российской Федерации.

- персональные данные Заемщика /потенциального Заемщика, а также персональные данные руководителя, участника (акционера) или сотрудника юридического лица, являющегося Заемщиком /потенциальным Заемщиком - информация, необходимая Обществу для выполнения своих договорных обязательств и осуществления прав в рамках соответствующего договора, заключенного с Заемщиком, для минимизации рисков Общества, связанных с нарушением обязательств по договору займа и для выполнения требований законодательства Российской Федерации.

2.4. В состав обрабатываемых в Обществе персональных данных субъекта входят паспортные данные (фамилия, имя, отчество, дата рождения, номер и серия паспорта, сведения о выдаче) и данные об адресе по месту жительства.

3. ЦЕЛИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

3.1. Общество осуществляет обработку персональных данных в следующих целях:

- осуществления деятельности, предусмотренной Уставом Общества, нормативными актами Банка России, действующим законодательством РФ, в частности ФЗ: «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных»;

- заключения, исполнения и прекращения гражданско-правовых договоров с физическими, юридическим лицами, индивидуальными предпринимателями и иными лицами, в случаях, предусмотренных действующим законодательством и Уставом Общества;

- организации кадрового учета Общества, обеспечения соблюдения законов и иных нормативно-правовых актов, заключения и исполнения обязательств по трудовым и гражданско-правовым договорам; ведения кадрового делопроизводства, содействия работникам в трудоустройстве, обучении и продвижении по службе, пользования различного вида льготами, исполнения требований налогового законодательства в связи с исчислением и уплатой налога на доходы физических лиц, а также единого социального налога, пенсионного законодательства при формировании и представлении персонифицированных данных о каждом получателе доходов, учитываемых при начислении страховых взносов на обязательное пенсионное страхование и обеспечение, заполнения первичной статистической документации, в соответствии с Трудовым кодексом РФ, Налоговым кодексом РФ, федеральными законами, в частности: «Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования», «О персональных данных», а также Уставом Общества.

4. СРОКИ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

4.1 Сроки обработки персональных данных определяются в соответствие со сроком действия договора с субъектом персональных данных, Приказом Минкультуры РФ от 25.08.2010 № 558 «Об утверждении «Перечня типовых управленческих архивных документов, образующихся в процессе деятельности государственных органов, органов местного самоуправления и организаций, с указанием сроков хранения», Постановлением ФКЦБ РФ от 16.07.2003 № 03-33/пс «Об утверждении Положения о порядке и сроках хранения документов акционерных обществ», сроком исковой давности, а также иными требованиями законодательства РФ и нормативными документами Банка России.

4.2 В Обществе создаются и хранятся документы, содержащие сведения о субъектах персональных данных. Требования к использованию в Обществе данных типовых форм документов установлены Постановлением Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».

5. ПРАВА И ОБЯЗАННОСТИ

5.1. Права и обязанности Общества.

5.1.1 Общество как оператор персональных данных, вправе:

- отстаивать свои интересы в суде;
- предоставлять персональные данные субъектов третьим лицам, если это предусмотрено действующим законодательством (налоговые, правоохранительные органы и др.);
- отказывать в предоставлении персональных данных в случаях предусмотренных законодательством;
- использовать персональные данные субъекта без его согласия, в случаях предусмотренных законодательством.

5.2. Права и обязанности субъекта персональных данных

5.2.1 Субъект персональных данных имеет право:

- требовать уточнения своих персональных данных, их блокирования или уничтожения в случае, если персональные данные являются неполными, устаревшими, недостоверными, незаконно полученными или не являются необходимыми для заявленной цели обработки, а также принимать предусмотренные законом меры по защите своих прав;
- требовать перечень своих персональных данных, обрабатываемых Обществом и источник их получения;
- получать информацию о сроках обработки своих персональных данных, в том числе о сроках их хранения;
- требовать извещения всех лиц, которым ранее были сообщены неверные или неполные его персональные данные, обо всех произведенных в них исключениях, исправлениях или дополнениях;
- обжаловать в уполномоченный орган по защите прав субъектов персональных данных или в судебном порядке неправомерные действия или бездействия при обработке его персональных данных;
- на защиту своих прав и законных интересов, в том числе на возмещение убытков и (или) компенсацию морального вреда в судебном порядке.

6. ПРИНЦИПЫ И УСЛОВИЯ ОБРАБОТКИ ПЕРСОНАЛЬНЫХ ДАННЫХ

6.1. Обработка персональных данных Обществом осуществляется на основе принципов:

- законности и справедливости целей и способов обработки персональных данных;
- соответствия целей обработки персональных данных целям, заранее определенным и заявленным при сборе персональных данных, а также полномочиям Общества;
- соответствия объема и характера обрабатываемых персональных данных, способов обработки персональных данных целям обработки персональных данных;

- достоверности персональных данных, их достаточности для целей обработки, недопустимости обработки персональных данных, избыточных по отношению к целям, заявленным при сборе персональных данных;

- недопустимости объединения созданных для несовместимых между собой целей баз данных, содержащих персональные данные;

- хранения персональных данных в форме, позволяющей определить субъекта персональных данных, не дольше, чем этого требуют цели их обработки;

- уничтожения по достижении целей обработки персональных данных или в случае утраты необходимости в их достижении.

6.2. Обработка персональных данных осуществляется на основании условий, определенных законодательством Российской Федерации.

7. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ

7.1 Общество предпринимает необходимые организационные и технические меры для обеспечения безопасности персональных данных от случайного или несанкционированного доступа, уничтожения, изменения, блокирования доступа и других несанкционированных действий.

7.2 В целях координации действий по обеспечению безопасности персональных данных в Обществе назначен ответственный за обеспечение безопасности персональных данных.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1 Настоящая Политика является внутренним документом Общества, общедоступной и подлежит размещению на официальном сайте Общества.

8.2 Настоящая Политика подлежит изменению, дополнению в случае появления новых законодательных актов и специальных нормативных документов по обработке и защите персональных данных, но не реже одного раза в три года.

8.3 Контроль исполнения требований настоящей Политики осуществляется ответственным за обеспечение безопасности персональных данных Общества.

8.4 Ответственность должностных лиц Общества, имеющих доступ к персональным данным, за невыполнение требований норм, регулирующих обработку и защиту персональных данных, определяется в соответствии с законодательством Российской Федерации и внутренними документами Общества.

ПРИЛОЖЕНИЕ Г

Общество
с ограниченной ответственностью
микрофинансовая организация
«ГОРОДСКОЙ ЗАЙМ»

ИНН 5607043734, КПП 560701001, ОГРН 11156580009114, ОКПО 90485194
462371, Оренбургская область, г. Новотроицк, пгт. Аккермановка, ул. Восточная, 1А
Телефон: 66-05-11, 8-903-3699016

АКТ
определения необходимого
уровня защищенности
персональных данных

УТВЕРЖДАЮ
Директор
ООО МФО «Городской Займ»
_____С.Т.Искулов
Дата_____

Акт определения необходимого уровня защищенности персональных данных, обрабатываемых в информационной системе персональных данных «Клиенты»

Комиссия по персональным данным, созданная в ООО МФО «Городской Займ» (далее по тексту – Общество) в составе:

Председатель комиссии:_____ _____
должность, Ф.И.О. подпись

Члены комиссии:_____ _____
должность, Ф.И.О. подпись

_____ _____
должность, Ф.И.О. подпись

_____ _____
должность, Ф.И.О. подпись

с целью
самостоятельной экспертной оценки необходимого уровня защищенности персональных данных, обрабатываемых в информационных системах персональных данных Общества,
рассмотрев
результаты по сбору и анализу исходных данных на информационную систему персональных данных (далее по тексту - ИСПДн) Общества, представленные в Паспорте организации с точки зрения информационной безопасности,
на основании
- того, что в Паспорте организации с точки зрения информационной безопасности была выделена информационная система персональных данных, названная для внутренней идентификации «Клиенты» (ИСПДн «Клиенты»);

- Модели угроз и уязвимостей для ИСПДн «Клиенты»,
во исполнение требований
Постановления Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» (далее Постановление Правительства №1119),
и пункта 5 части 1 статьи 181 Федерального закона № 152-ФЗ от 27 июля 2006 года «О персональных данных»,
в соответствии с нормой
пункта 7. Постановления Правительства № 1119 о том, что определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом проведенной Обществом оценки возможного вреда, определила:

1. ИСПДн «Клиенты» является информационной системой, обрабатывающей иные категории персональных данных, так как в ИСПДн не обрабатываются персональные данные, относящиеся к специальной категории ПДн (персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни субъектов ПДн), или к биометрическим персональным данным (ПДн, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность и которые используются оператором для установления личности субъекта ПДн), или к общедоступным персональным данным (ПДн, полученные только из общедоступных источников персональных данных, созданных в соответствии со статьей 8 Федерального закона «О персональных данных»).
2. ИСПДн «Клиенты» является информационной системой, обрабатывающей персональные данные в объеме менее 100.000.
3. Для ИСПДн актуальны угрозы 3-го типа, так как для данной ИСПДн не актуальны угрозы, связанные с наличием недокументированных возможностей в прикладном и системном программном обеспечении.
4. ИСПДн «Клиенты» является информационной системой, обрабатывающей иные категории персональных данных субъектов персональных данных, не являющихся работниками Общества.
5. ИСПДн «Клиенты», по заданным характеристикам безопасности, относится к специальным информационным системам, в которых требуется обеспечение конфиденциальности, доступности и целостности персональных данных.
6. По структуре ИСПДн «Клиенты» представляет собой не распределенную информационную систему, состоящую из автоматизированного рабочего места, представляющего собой информационную систему работающую без использования технологий удаленного доступа.
7. ИСПДн «Клиенты» не имеет подключения к сетям международного информационного обмена.

8. В ИСПДн «Клиенты» обработка персональных данных осуществляется с разграничением прав доступа пользователей.

9. Весь аппаратный комплекс и рабочие места ИСПДн «Клиенты» находятся в пределах Российской Федерации.

ВЫВОД: По результатам проведенного анализа, и, исходя из того, что для информационной системы персональных данных «Клиенты» актуальны угрозы 3-го типа, и в ней обрабатываются иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся работниками Общества, комиссия пришла к заключению, что для ИСПДн «Клиенты» необходимо обеспечить 4-й уровень защищенности персональных данных при их обработке в информационной системе.

Комиссия устанавливает, что для обеспечения 4-го уровня защищенности персональных данных при их обработке в ИСПДн «Клиенты» необходимо выполнение следующих требований:

а) организация режима обеспечения безопасности помещений, в которых размещена ИСПДн, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

б) обеспечение сохранности носителей персональных данных;

в) утверждение Генеральным директором Общества документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в ИСПДн, необходим для выполнения ими трудовых обязанностей;

г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.

Председатель комиссии:_____ _____
должность, Ф.И.О. подпись

Члены комиссии:_____ _____
должность, Ф.И.О. подпись

_____ _____
должность, Ф.И.О. подпись

_____ _____
должность, Ф.И.О. подпись

«___» _____ 201_ года

ПРИЛОЖЕНИЕ Д

Общество
с ограниченной ответственностью
микрофинансовая организация
«ГОРОДСКОЙ ЗАЙМ»

ИНН 5607043734, КПП 560701001, ОГРН 11156580009114, ОКПО 90485194
462371, Оренбургская область, г. Новотроицк, пгт. Аккермановка, ул. Восточная, 1А
Телефон: 66-05-11, 8-903-3699016

ТЕХНИЧЕСКОЕ ЗАДАНИЕ
на создание системы защиты
информационной системы
персональных данных

УТВЕРЖДАЮ
Директор
ООО МФО «Городской Займ»
_____С.Т.Искулов
Дата_____

Информационная система персональных данных
ООО МФО «Городской Займ»

ТЕХНИЧЕСКОЕ ЗАДАНИЕ

На 5 листах

СОГЛАСОВАНО
Директор
ООО МФО «Городской Займ»
_____С.Т.Искулов
Дата_____

1. ОБЩИЕ СВЕДЕНИЯ

1.1. Полное наименование системы и ее условное обозначение

Информационная система персональных данных ООО МФО «Городской Займ» (далее – ИСПДн).

1.2. Наименование заказчика и исполнителя

Предприятие заказчик системы: ООО МФО «Городской Займ»
Предприятие исполнитель системы: ООО МФО «Городской Займ»

1.3. Перечень документов, на основании которых создается ИСПДн

1.3.1. Нормативная база, регулирующая сферу ЗИ

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ № 687 от 15.09.2008 г. «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;
- Руководящий документ ФСТЭК России «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Руководящий документ ФСТЭК России «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных»;
- ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания»;
- ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем»;
- ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения».

1.3.2. Нормативная база, регулирующая сферу деятельности организации

- Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Комплекс документов Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации»;
- Федеральный закон от 02.07.2010 N 151-ФЗ "О микрофинансовой деятельности и микрофинансовых организациях";

- Федеральный закон от 21.12.2013 N 353-ФЗ "О потребительском кредите (займе)";
- Федеральный закон от 07.08.2001 N 115-ФЗ "О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма";
- Приказ Минфина РФ от 03.03.2011 N 26н "Об утверждении Порядка ведения государственного реестра микрофинансовых организаций";
- Приказ Минфина России от 01.03.2012 № 37н "Об утверждении форм и сроков представления документов, содержащих отчет о микрофинансовой деятельности и персональном составе руководящих органов микрофинансовой организации".

1.4. Порядок оформления и предоставления результатов работ по созданию системы

Порядок определяется на основании действующих стандартов и договорных документов между Заказчиком и Исполнителем.

Результаты работы оформляются и предъявляются заказчику по мере исполнения в виде минимальных независимых частей проекта и/или предварительных проектов.

2. НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1. Назначение системы

Назначением системы является обеспечение конфиденциальности и информационной безопасности ПДн, обрабатываемых в ИСПДн.

2.2. Цели создания системы

Целью создания системы является обеспечение конфиденциальности и защищенности ИСПДн в процессе обработки и хранения ПДн, в также соответствие требованиям обеспечения ИБ при обработке ПДн в ИСПДн, регламентируемых РД ФСТЭК и ФСБ России.

3. ХАРАКТЕРИСТИКА ОБЪЕКТОВ ЗАЩИТЫ

3.1. Краткие сведения об объектах защиты

Объектами защиты являются персональные данные, средства их обработки и хранения, а также помещения, в которых расположена ИС.

Средства обработки:

- АРМ руководства;
- АРМ сотрудников.

Носители информации:

- бумажные носители информации;
- электронные носители.

Персонал:

- руководитель;
- сотрудники.

Помещения:

- помещение отдела для работы с клиентами.

4. ТРЕБОВАНИЯ К ИСПДН

4.1. Требования законодательства

В соответствии с Приказом ФСТЭК России от 18 февраля 2013 г. N 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», в состав мер по обеспечению безопасности персональных данных входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

5. СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО РАЗРАБОТКЕ

5.1. Структура выполнения работ

ИСПДн 1. Проектирование

ИСПДн 1.1. Определение текущих бизнес-процессов

ИСПДн 1.2. Анализ проблем текущих бизнес-процессов

ИСПДн 1.3. Разработка значений ключевых показателей новых бизнес-процессов

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

ИСПДн 1.5. Разработка и согласование структуры новых бизнес-процессов

ИСПДн 2. Совершенствование организационно распорядительной документации

ИСПДн 2.1. Политика в отношении обработки ПДн

ИСПДн 2.2. Внесение изменений в должностные инструкции сотрудников

ИСПДн 2.3. Согласование и утверждение документации

ИСПДн 3. Подготовка реализации проекта

ИСПДн 3.1. Определение ответственных лиц и исполнителей проекта

ИСПДн 3.2. Приобретение антивирусного ПО

ИСПДн 3.3. Приобретение средства защиты от НСД

ИСПДн 4. Внедрение

ИСПДн 4.1. Установка и настройка антивирусного ПО

ИСПДн 4.2. Установка и настройка средств защиты от НСД

ИСПДн 4.3. Контроль защищенности

ИСПДн 4.4 Обучение пользователей.

6. ПОРЯДОК КОНТРОЛЯ И ПРИЕМКИ

6.1. Критерии оценивания работ

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

6.2. Порядок приемки

Приемка работ осуществляется единовременно.

6.3. Порядок оформления замечаний

Заказчик направляет замечания в письменном виде.

7.ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ВВОДУ ИСПДН В ЭКСПЛУАТАЦИЮ

7.1. Должен быть определен перечень лиц, допущенных к обработке ПДн, обрабатываемых в ИСПДн.

7.2. Должен быть определен перечень информации, классифицируемой как ПДн.

7.3. Разграничение прав доступа в защищаемые помещения должно регламентироваться внутренними организационно-распорядительными документами организации.

7.4. Компоненты ИСПДн должны быть подключены к источникам бесперебойного питания.

7.5. Серверное помещение должно быть оборудовано средствами вентиляции и кондиционирования воздуха, достаточными для работы оборудования в соответствии с документацией производителя, а также средствами автоматического пожаротушения и пожарной сигнализации.

8. ТРЕБОВАНИЯ К ДОКУМЕНТАЦИИ

8.1. Перечень документов, которые должны быть разработаны

В соответствии с ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем» рекомендуется выпустить следующий комплект документации:

- Ведомость эскизного проекта;
- Пояснительная записка к эскизному проекту;
- Описание технологического процесса обработки данных;
- Таблица соединений и подключений;
- План расположения;
- Технологическая инструкция;
- Руководство пользователя;
- Общее описание системы;
- Программа и методика испытаний
- Паспорт.

8.2 Порядок предоставления документов

Комплект документов предоставляется предприятию заказчику в электронном виде и бумажной копии.