МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра Прикладная математика и информатика
(наименование)

09.03.03 Прикладная информатика
(код и наименование направления подготовки, специальности)

Бизнес-информатика
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему Разработка политики информационной безопасности отделения срочного социального обслуживания (на примере МКУ «ЦСОГПВиИ Таштагольского г.п.»)

Студент А.А. Судаков
(И.О. Фамилия) (личная подпись)

Руководитель кандидат педагогических наук, доцент, Е.В. Панюкова
(ученая степень, звание, И.О. Фамилия)

Тольятти 2020

Аннотация

Выпускная квалификационная работа посвящена вопросу по разработке политики информационной безопасности отделения срочного социального обслуживания (на примере МКУ «ЦСОГПВиИ Таштагольского г.п.»).

Целью работы является разработка политики информационной безопасности отделения срочного социального обслуживания (на примере МКУ «ЦСОГПВиИ Таштагольского г.п.») от несанкционированного доступа третьих лиц.

Данная работа состоит из введения, трех глав, заключения, списка литературы и приложений.

Во введении представлена актуальность темы, определены цель и задачи, объект и предмет исследования.

В первой главе приведен анализ деятельности учреждения. Приведена информация об организационной структуре, показана структура бизнес-процессов учреждения.

Во второй главе были рассмотрены вопросы разработки политики информационной безопасности.

В третьей главе был рассмотрен вопрос экономического обоснования внедрения политики информационной безопасности.

В заключении представлены выводы по проделанной работе.

Результатом работы является разработанная политика информационной безопасности отделения срочного социального обслуживания (на примере МКУ «ЦСОГПВиИ Таштагольского г.п.») от несанкционированного доступа третьих лиц.

В работе представлено 15 таблиц, 10 рисунков, 4 приложения, список использованной литературы содержит 30 источников. Общий объем выпускной квалификационной работы составляет 69 страниц.

Оглавление

Введение

Темой выпускной квалификационной работы является разработка политики информационной безопасности отделения срочного социального обслуживания на примере муниципального казенного учреждения «Центр социального обслуживания граждан пожилого возраста и инвалидов Таштагольского городского поселения» (далее – МКУ «ЦСОГПВиИ Таштагольского г.п.»).

Специфика работы социальной сферы имеет ряд важных особенностей:

1. Бюджетная основа организации.
2. Социальный статус контингента людей (пенсионеры, инвалиды, ветераны, вдовы, погорельцы, пострадавшие от паводка, малообеспеченные, семьи с детьми, маломобильные граждане и т.д.).
3. Контроль за оказанием адресной помощи гражданам, которые оказались в трудной жизненной ситуации.

Использование информационных технологий в социальной сфере является неотъемлемым условием для реализации Федеральных Законов об оказании адресной помощи. Любая информация в организациях подлежит защите и нераспространению. Информационные системы обеспечивают жизнеспособность организаций любого масштаба, в том числе и в сфере социальной защиты населения. Это обусловлено в первую очередь большой производительностью и доступным функционалом современных информационных систем, и низкой ценой, что является огромным плюсом в связи с ограниченным бюджетом муниципальных казенных учреждений [1].

Разработка эффективной политики информационной безопасности обеспечивает безопасность баз данных клиентов, предоставляет возможность составления прогнозов эффективности, выявление ошибок сотрудников, решения задач управления и планирования деятельности.

В связи с непростой экономической ситуацией в стране, невзирая на экономические санкции, реализуется процесс импортозамещения –

повсеместно проходит оцифровывание бизнес-процессов социальной защиты населения с использованием отечественных и бюджетных разработок.

Все чаще требуются квалифицированные специалисты в области создания, внедрения и организации защиты информации в информационных системах учреждений.

Объектом исследования в рамках выполнения выпускной квалификационной работы выступает отделение срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

Предмет исследования – организация политики информационной безопасности отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

Целью выпускной квалификационной работы является разработка политики информационной безопасности от несанкционированного доступа третьих лиц отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

В рамках выполнения выпускной квалификационной работы задачами для достижения поставленной цели выступают:

- исследование имеющейся системы информационной безопасности;
- анализ и выявление нарушений в защите информационной безопасности, а также выявление наиболее вероятных угроз информации;
- разработка новых мер по обеспечению системы информационной безопасности – политика информационной безопасности;
- разработка частной модели угроз на примере информационной системы «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»);
- разработка документации по информационной безопасности;
- внедрение программных и аппаратно-технических средств защиты в отделении срочного социального обслуживания.

Глава 1 Анализ предметной области

1.1 Сфера деятельности и характеристика учреждения

Муниципальное казённое учреждение «Центр социального обслуживания граждан пожилого возраста и инвалидов Таштагольского городского поселения» (далее – Учреждение), создано на основании ст.ст. 296; 297; 298 Гражданского кодекса Российской Федерации, Федерального закона от 08.05.2010 г. № 83-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием правового положения государственных учреждений» (с изменениями от 27.11.2017г.)[11], в соответствии с постановлением администрации Таштагольского района от 07.12.2010 года № 1028-п «Об утверждении порядка принятия решения о создании, реорганизации, изменении типа и ликвидации муниципальных учреждений Таштагольского района, а также утверждение уставов муниципальных учреждений Таштагольского района и внесения в них изменений»[12], постановлением администрации Таштагольского муниципального района № 500-п от «09» июня 2014 года «О реорганизации муниципального казенного учреждения «Центр социального обслуживания граждан пожилого возраста и инвалидов» Шерегешского городского поселения путем присоединения к Муниципальному казенному учреждению «Центр социального обслуживания граждан пожилого возраста и инвалидов Таштагольского городского поселения».

Учреждение является некоммерческой организацией. В своей деятельности учреждение руководствуется Конституцией РФ, Федеральным законом от 28.12.2013г. № 442 «Об основах социального обслуживания граждан в Российской Федерации» (с изменениями от 07.03.2018г.) [10] и другими федеральными законами, постановлениями и распоряжениями Правительства РФ, нормативно правовыми актами Минтруда России, Департамента социальной защиты населения Кемеровской области,

Администрации Таштагольского муниципального района и отраслевого (функционального) органа администрации Таштагольского муниципального района – муниципального казённого учреждения «Управление социальной защиты населения администрации Таштагольского муниципального района», Уставом МКУ «ЦСОГПВиИ Таштагольского г.п.»[13], Положением о МКУ «ЦСОГПВиИ Таштагольского г.п.»[9].

Официальное полное наименование Учреждения: Муниципальное казённое учреждение «Центр социального обслуживания граждан пожилого возраста и инвалидов Таштагольского городского поселения». Сокращенное наименование Учреждения: МКУ «ЦСОГПВиИ Таштагольского г.п.». Учредителем и собственником имущества Учреждения является Администрация Таштагольского муниципального района.

Основными задачами деятельности Центра являются:

− по заранее разработанным регламентам и критериям выявлять граждан, которые потенциально нуждаются в социальной помощи или находятся в тяжелой жизненной ситуации;

− в соответствии с регламентами учреждения проводить политику предупреждения или снижения уровня зависимости граждан от социальной помощи. Консультировать и способствовать в поисках работы, выдаче б/у вещей в пунктах обмена, помощь в оформлении официальных документов;

− выявлять и определять категории граждан нуждающихся в социальном обеспечении на дому в стационарных условиях. К таким гражданам можно отнести людей, имеющие проблемы со здоровьем – малоподвижные, инвалиды, слепые, глухонемые и т.д.;

− оказание социально-бытовых, социально-правовых, социально-психологических услуг в целях повышения коммуникативного потенциала получателей социальных услуг, имеющих ограничения жизнедеятельности и иных услуг постоянного, временного или разового характера гражданам, нуждающимся в социальном обслуживании, в соответствии со стандартами социальных услуг утвержденных Постановлением Коллегии Администрации

КО от 22.12.2014 № 515 «Об утверждении порядков предоставления социальных услуг на дому, в полустационарной форме социального обслуживания и срочных социальных услуг»[14];

− обеспечить постоянный контроль и мониторинг за нововведениями в сфере социальной защиты;

− искать способы решения возникающих проблем с привлечением волонтерских организаций или коммерческих структур по содействию проведения общественных мероприятий;

− ежегодная аттестация навыков и знаний работников, содействие в получении дополнительного образования по специальности, проведение курсов.

Зачисление граждан на социальное обслуживание происходит на основе заявления и других документах, поданных в установленный срок, установленный законодательством РФ. Основания для отказа в социальном обслуживании граждан закреплены в законодательстве РФ и нормативно-правовых актах локального типа администрации или на уровне департамента социальной службы населения.

МКУ «ЦСОГПВиИ Таштагольского г.п.» состоит из следующих подразделений:

− отделения социальной помощи на дому №1 - №5;

− отделение срочного социального обслуживания №1;

− административно-хозяйственная часть (АХЧ).

На заведование каждым отделением в МКУ «ЦСОГПВиИ Таштагольского г.п.» назначается заведующая, в соответствии с приказом директора. Контроль над деятельностью всех отделений осуществляет директор учреждения. Организационная структура Центра социального обслуживания (МКУ «ЦСОГПВиИ Таштагольского г.п.») указана в соответствии с рисунком 1.1.

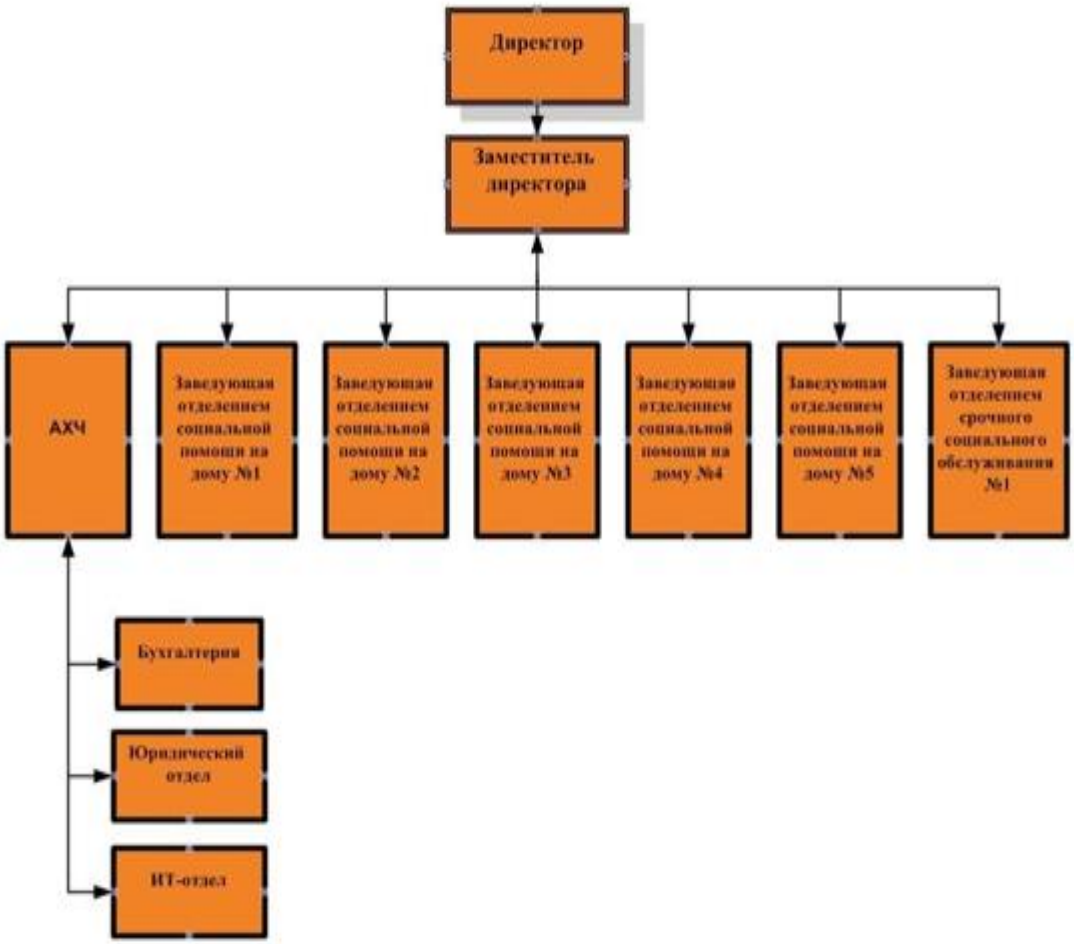

Рисунок 1.1 – Организационная структура

Описание подразделений по указанным подразделениям:

− директор. Выполняет руководство организацией, решает все вопросы.

− административно-хозяйственная часть (АХЧ). В данное подразделение входит заместитель директора, отдел бухгалтерии, специалист по кадрам, IT-отдел, завхоз, экономический отдел, инженер по охране труда, юридический отдел. Подчиняются и выполняют непосредственные указания директора по кадровой политике, организации выплат, бесперебойной работы инфокоммуникационной системы предприятия, охране труда и безопасности рабочих мест в соответствии с законодательством РФ.

− отделение срочного социального обслуживания. В данном подразделении работают заведующая и специалисты по социальной работе.

Осуществляют прием клиентов по их обращениям, выдают консультации и проводят аналитическую работу.

− отделение социальной помощи на дому№1, отделение социальной помощи на дому№2, отделение социальной помощи на дому№3. В данных подразделениях осуществляют свою трудовую деятельность заведующие социальной помощи на дому по городскому сектору, по частному сектору в черте города и по сельским территориям. Осуществляют прием клиентов по их обращениям, выдают консультации и проводят аналитическую работу.

На основе анализа организационной структуры и трудовых функций персонала за основу будет взята работа отделения срочного социального обслуживания, на базе которой будет разработана политика информационной безопасности.

1.2 Анализ и оценка защиты данных в активах отделения срочного социального обслуживания

В соответствии с рисунком 1.2 представлена контекстная IDEF0-диаграмма процесса защиты информации в отделении социального обслуживания.

Рисунок 1.2 – Контекстная IDEF0-диаграмма организации СЗИ в информационных системах «КАК ЕСТЬ» (0-й уровень)

На выходе из процесса – защищаемая информация отдела.

1.2.1 Идентификация информации, циркулирующей в отделении

В рамках выполнения выпускной квалификационной работы необходимо провести анализ информации на защищаемом объекте – отделение срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.». Благодаря данному анализу актива можно выявить перечень источников, которые могут потерять полностью или частично свойства информационной безопасности при реализации угроз потенциальными нарушителями: доступность, целостность и конфиденциальность.

В отделении срочного социального обслуживания не обрабатывается информация, содержащая государственную тайну. В таблице 1.1 отражен перечень источников и носителей конфиденциальной информации.

Таблица 1.1 – Перечень источников и носителей информации

№	Наименование элемента информации	Тип информации	Источники информации	Расположение
1.	Журналы	ПД	Сотрудники, документация	Отделение срочного социального обслуживания
2.	Карточки	ПД	Сотрудники, документация	Отделение срочного социального обслуживания
3.	Акты обследования	ПД	Сотрудники, документация, ТСОИ	Отделение срочного социального обслуживания
4.	Служебные записки	КТ	Сотрудники, документация, ТСОИ	Кабинеты руководителей
5.	Отчеты	КТ	Сотрудники, документация, ТСОИ	Отделение срочного социального обслуживания, кабинеты руководителей
6.	Документация (приказы, регламенты)	КТ	Сотрудники, документация, ТСОИ	Кабинеты руководителей
7.	Электронная база данных	ПД	Сотрудники, документация, ТСОИ	Отделение срочного социального обслуживания, кабинет администратора ИБ.

Обозначения: ПД – персональные данные, КТ – коммерческая тайна,

ТСОИ – техническое средство обработки информации.

1.2.2 Идентификация аппаратного и программного обеспечения в отделении срочного социального обслуживания

В работе отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.» используются следующие информационные системы персональных данных (далее – ИСПДн):

1. Информационная система «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»). Удобный интерфейс, многозадачный, интегрирован с другими системами.

2. Автоматизированная информационная система на базе табличного процессора LibreOffice Calc (бесплатный аналог MS Office Excel). Не обладает достаточной функциональностью для ведения учета услуг в Центре социального обслуживания. Используется для составления отчетов (недельные, квартальные, годовые).

3. Автоматизированная информационная система на базе текстового процессора LibreOffice Writer (бесплатный аналог MS Office Word). Используется для составления актов обследования жилищно-бытовых условий. В таблице 1.2 отражен анализ аппаратного и программного обеспечения в отделении срочного социального обслуживания.

Таблица 1.2 – Анализ аппаратного и программного обеспечения

№	Техническое/программное обеспечение	Количество
Техническое обеспечение		
1.	Автоматизированное рабочее место (АРМ)	5
2.	Многофункциональное устройство (МФУ)	2
3.	Свитч	2
4.	Внешние устройства хранения данных (флеш-накопители, мобильные телефоны).	5
5.	Локально-вычислительная сеть (ЛВС) Общие сетевые папки	1

Продолжение таблицы 1.2 – Анализ аппаратного и программного обеспечения

Программное обеспечение		
1.	Офисный пакет LibreOffice	5
2.	Операционная система семейства Windows (7 и 10)	5
3.	Информационная система «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»).	5
4.	Антивирусное ПО – Avast Free Antivirus	5
5.	Веб-обозреватель Mozilla Firefox 72 и Internet Explorer 11	5

В выпускной квалификационной работе при разработке политики информационной безопасности для примера составления частной модели угроз безопасности персональных данных будет рассмотрена информационная система «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»).

1.2.3 Идентификация услуг, предоставляемых отделением срочного социального обслуживания

Процедура идентификации бизнес-процессов Центра социального обслуживания на примере отделения срочного социального обслуживания заключалась в том, чтобы выделить только ключевые процессы. Идентификация бизнес-процессов отделения срочного социального обслуживания проводилась на основе теоретических знаний по моделированию бизнес-процессов и личным опытом работы в учреждении.

Основными задачами отделения срочного социального обслуживания являются:

− выявление и учет граждан, остро нуждающихся в социальной помощи;

− принятие безотлагательных мер и оказание экстренной социальной

помощи, направленных на поддержание жизнедеятельности граждан, остро нуждающихся в социальной поддержке, в связи с возникновением трудной жизненной ситуации;

− определение конкретных форм помощи гражданам, исходя из состояния их здоровья, возможности к самообслуживанию и конкретной жизненной ситуации;

− содействие в обеспечении граждан, попавших в трудную жизненную ситуацию, одеждой, обувью, другими предметами первой необходимости и бесплатными продуктами питания;

− распределение среди нуждающихся граждан товаров, поступающих по линии гуманитарной помощи;

− организация социальной поддержки граждан, нуждающихся в социальном обслуживании на дому, на период до зачисления их в отделения социальной помощи на дому или помещения их в дом – интернат, палаты сестринского ухода, больницы;

− помощь в сборе документов и в оформлении в дома-интернаты, палаты сестринского ухода, больницы;

− оказание других форм срочной социальной помощи;

− организация дополнительных услуг.

Документы и иные сущности, используемые при исполнении моделируемых бизнес-процессов и необходимые для моделирования документооборота, с описаниями их основного смысла, следующие:

1. Нормативно-правовые документы.

Регламент «Методика организации и проведения работы отделения срочного социального обслуживания», приказы, распоряжения, положения – основа нормативной базы отделения.

В своей деятельности Центр социального обслуживания руководствуется федеральным законом от 28.12.2013г. № 442 «Об основах социального обслуживания граждан в Российской Федерации» (с изменениями от 07.03.2018г.) [8]. На основе данного закона в отделении

срочного социального обслуживания был разработан регламент «Методика организации и проведения работы отделения срочного социального обслуживания» [15]. Контроль над исполнением методики осуществляется путем анализа статистических отчетов по регламентируемым формам.

2. Обращения клиентов за адресной социальной помощью.

Заявления клиентов, журнал приема посетителей.

Социальные услуги предоставляются гражданам на основании документа, удостоверяющего их личность, и письменного заявления по форме, утвержденной приказом Министерства труда и социальной защиты Российской Федерации от 28.03.2014 № 159н «Об утверждении форм заявления о предоставлении социальных услуг» [16].

Все обращения граждан регистрируются в журнале приёма посетителей, далее вносятся в табличные формы LibreOffice (бесплатный аналог MS Office).

3. Статистические отчеты.

Для передачи отчетов в вышестоящие организации создаются дополнительные табличные формы для ведения статистики получателей социальных услуг.

Отчеты составляются строго по разработанным формам.

4. Договора.

С клиентами заключаются договора о предоставлении услуг по прокату технических средств реабилитации.

Структура бизнес-процессов, отражающая их иерархию от более общих групп к частным бизнес-процессам на примере отделения срочного социального обслуживания и отделений социальной помощи на дому (для сравнения) указана в соответствии с рисунком 1.3.

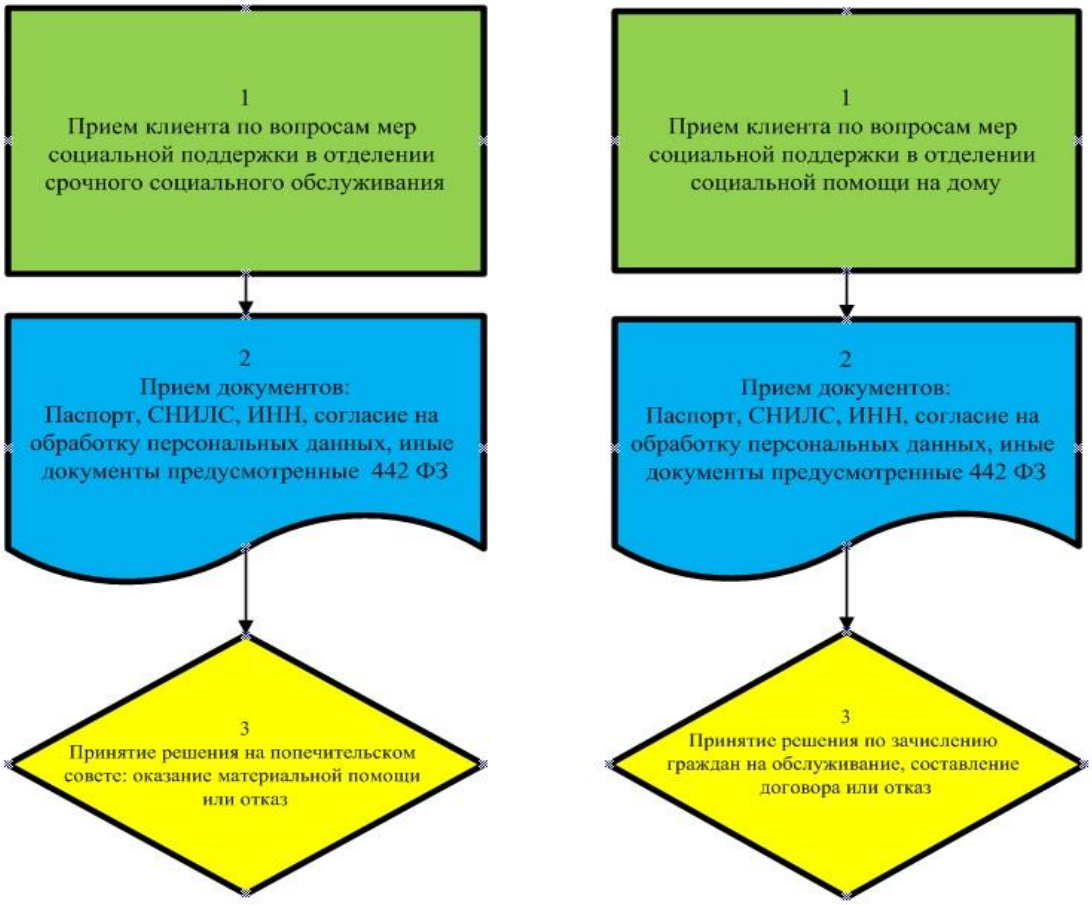

Рисунок 1.3 – Схема структуры бизнес-процессов в МКУ «ЦСОГПВиИ Таштагольского г.п.»

В результате проведенного анализа работы отделения срочного социального обслуживания мною было выделено 3 группы бизнес-процессов:

- основные процессы;
- вспомогательные процессы;
- процесс управления.

Всего было выделено 8 бизнес-процессов.

Классификация процессов представлена в соответствии с рисунком 1.4.

В основные процессы были включены 5 процессов:

- учет выполненных услуг – комплекс услуг, финансируемых из областного бюджета (благотворительный уголь, овощные наборы, страхование от паводка, материальная помощь, иная безотлагательная

помощь);

- оказание услуги «Социальное такси»;
- оказание услуги «Выдача средств реабилитации»;
- оказание услуги «Выдача б/у вещей»;
- оказание услуги «Составление заявки в дом-интернат».

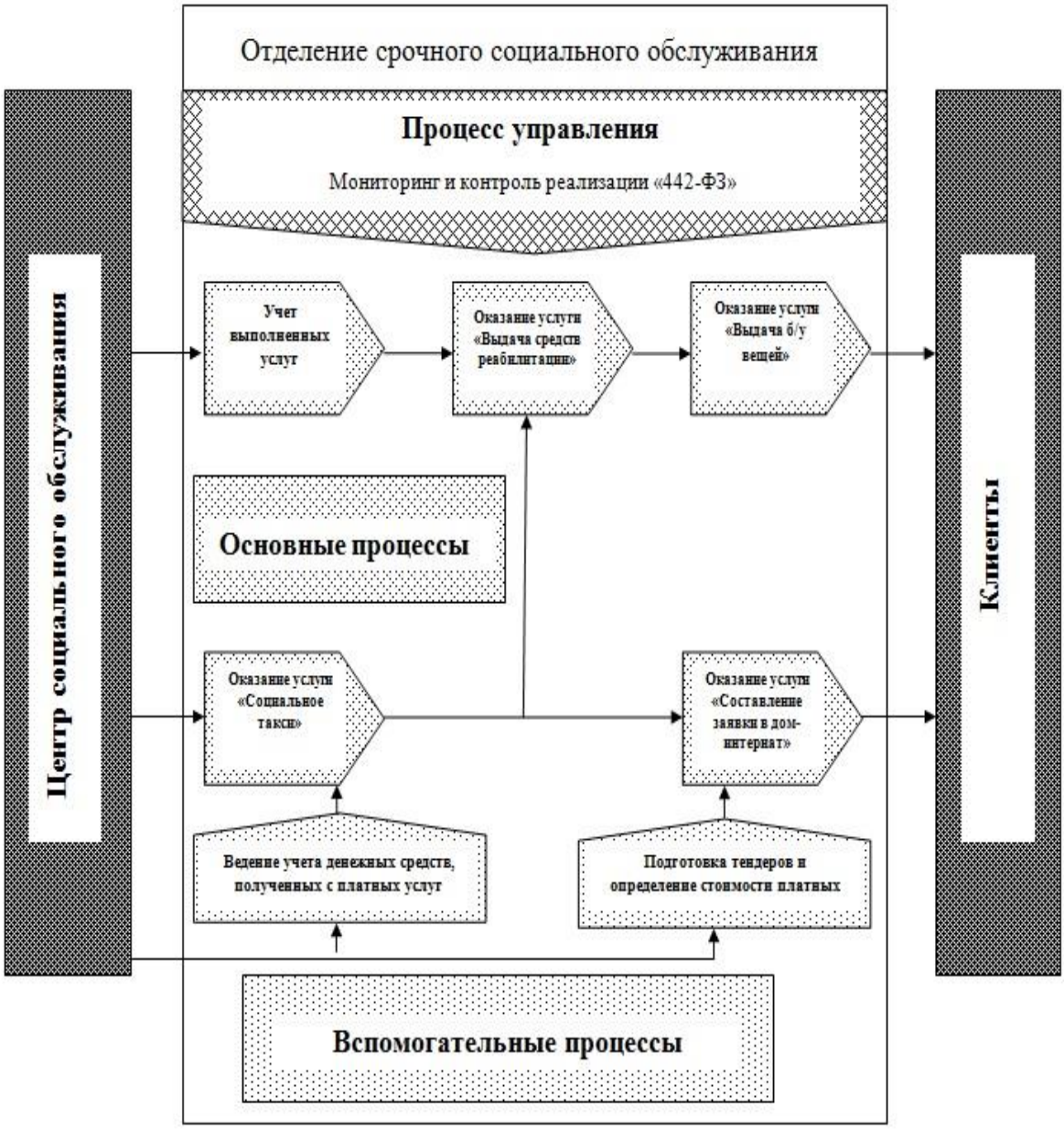

Рисунок 1.4 – Классификация бизнес-процессов отделения срочного социального обслуживания

Эти процессы составляют основу работы отделения срочного социального обслуживания, и помогают решать поставленные перед ней задачи по реализации 442-ФЗ «Об основах социального обслуживания граждан в Российской Федерации».

Вспомогательные процессы включают:

- Ведение учета денежных средств, полученных с платных услуг.
- Подготовка тендеров и определение стоимости платных услуг.

Эти процессы снабжают ресурсами деятельность отделения срочного социального обслуживания и обеспечивают работу основных процессов.

В процесс управления был включен – мониторинг и контроль реализации «442-ФЗ».

Выполнение этого бизнес-процесса обеспечивает управление отделением срочного социального обслуживания и регулирует текущую деятельность.

1.3 Анализ уязвимостей и угроз активов отделения срочного социального обслуживания

Перечень уязвимостей:

- уязвимость системного и прикладного программного обеспечения;
- неправильная настройка технических средств защиты и антивирусного программного обеспечения;
- несанкционированное использование «левых» программ, которые подгружают систему, нагружают ОЗУ;
- внедрение вирусов, программ-шпионов, плагинов;
- неумышленные действия пользователей ИСПДн;
- сбои аппаратно-технических средств.

В таблице 1.3 отражены результаты оценки уязвимостей активов.

Таблица 1.3 – Результаты оценки уязвимостей активов

Группа уязвимостей Содержание уязвимостей	Журналы	Карточки	Акты обследования	Служебные записки	Отчеты	Документация (приказы	Электронная база данных
1. Среда и инфраструктура							
Отсутствие ограничения физического доступа в помещение, кабинеты	средняя	средняя	средняя	низкая	средняя	низкая	низкая
Нестабильная работа электросети			низкая	низкая	низкая	низкая	низкая
2. Аппаратное обеспечение							
Сбои аппаратно-технических средств			низкая	низкая	низкая	низкая	низкая
Отсутствие контроля над изменением конфигураций оборудования			низкая	низкая	низкая	низкая	низкая
3. Программное обеспечение							
Уязвимость системного и прикладного программного обеспечения			низкая	низкая	низкая	низкая	средняя
Неправильная настройка технических средств защиты и антивирусного программного обеспечения			средняя	средняя	средняя	средняя	средняя
Несанкционированное использование «левых» программ, которые нагружают ОЗУ			низкая	низкая	низкая	низкая	средняя
Внедрение вирусов, программ-шпионов, плагинов			высокая	высокая	высокая	высокая	высокая

Продолжение таблицы 1.3 – Результаты оценки уязвимостей активов

4. Коммуникация							
Незащищенность линий связи			низкая	низкая	низкая	низкая	средняя
Отсутствие контроля над исполнителем	низкая	низкая	низкая	низкая	низкая	низкая	средняя
5. Документ (Документооборот)							
Неконтролируемое копирование, хранение информации	низкая	низкая	низкая	низкая	низкая	низкая	средняя
Хранение в незащищенном месте	низкая	низкая	низкая	низкая	низкая	низкая	низкая
6. Персонал							
Низкий уровень подготовки сотрудников по обеспечению ИБ	низкая	низкая	низкая	низкая	низкая	низкая	низкая
Неумышленные действия пользователей ИСПДн	низкая	низкая	низкая	низкая	низкая	низкая	низкая
7. Общие уязвимые места							
Низкое качество технического обслуживания			низкая	низкая	низкая	низкая	низкая

В таблице 1.4 отражены результаты оценки угроз активов.

Таблица 1.4 – Результаты оценки угроз активов

Группа угроз Содержание угроз	Журналы	Карточки	Акты обследования	Служебные записки	Отчеты	Документация (приказы,	Электронная база данных
1. Угрозы, обусловленные преднамеренными действиями							
Кража носителей информации	высокая	высокая	высокая	низкая	средняя	низкая	низкая
Разглашение информации, модификация и ее уничтожение, сотрудниками, допущенными к ее обработке	высокая	высокая	высокая	низкая	средняя	средняя	высокая

Продолжение таблицы 1.4 – Результаты оценки угроз активов

Несанкционированное отключение средств защиты			низкая	низкая	низкая	низкая	средняя
Действия вредоносных программ (вирусов)			высокая	высокая	высокая	высокая	высокая
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	низкая	низкая	низкая	низкая
Угрозы выявления паролей по сети			низкая	низкая	низкая	низкая	низкая
Угрозы подмены доверенного объекта в сети							низкая
Угрозы удаленного запуска приложений							средняя
Угрозы внедрения по сети вредоносных программ			средняя	средняя	средняя	средняя	средняя
2. Угрозы, обусловленные случайными действиями							
Угроза утечки видовой информации (текст, изображения и т.п.)	средняя	средняя	средняя	низкая	низкая	низкая	средняя
Утрата ключей и атрибутов доступа			низкая	низкая	низкая	низкая	низкая

Продолжение таблицы 1.4 – Результаты оценки угроз активов

Ошибки сотрудников	низкая	низкая	низкая	низкая	низкая	низкая	низкая
3. Угрозы, обусловленные естественными причинами							
Пожар, подтопление	низкая	низкая	низкая	низкая	низкая	низкая	низкая
Колебания напряжения	низкая	низкая	низкая	низкая	низкая	низкая	низкая

Перечень актуальных угроз: угрозы, обусловленные преднамеренными действиями; угрозы, обусловленные случайными действиями; угрозы, обусловленные естественными причинами (пожар, наводнения, колебания напряжения).

1.4 Анализ и оценка рисков активов отделения срочного социального обслуживания

В рамках выполнения выпускной квалификационной работы необходимо выявить всевозможные риски.

Для анализа активов системы информационной безопасности используется метод МАРИОН (MARION).

Метод является стандартом по определению компьютерных рисков. Соответствует стандарту ISO-SC27-WG1.

План методики Марион:

а. составление критериев оценки;

б. заполнение плана оценки.

Содержание оцениваемых активов:

1. Общая безопасность:

- 101. Общая организация.
- 102. Общий контроль.
- 103. Процедуры безопасности и аудит.

2. Социоэкономические факторы:

- 201. Социоэкономические факторы.

3. Общая компьютерная безопасность:

- 301. Окружение.
- 302. Контроль физического доступа.
- 303. Загрязнение.
- 304. Инструкции по безопасности.
- 305. Пожарная безопасность.
- 306. Безопасность от проникновения воды.
- 307. Правильность установки компьютеров.
- 308. Связь между пользователями и персоналом ИТ.
- 309. Кадровая политика отдела ИТ.
- 310. Стратегия ИТ.

4. Логический контроль доступа:

- 401. Безопасность аппаратного и системного ПО.
- 402. Безопасность телекоммуникаций.
- 403. Безопасность баз данных.

5. Безопасность операций:

- 501. Сохранение и восстановление данных.
- 502. Подготовка и передача данных.
- 503. Резервное копирование.
- 504. Поддержка аппаратного и программного обеспечения.

По данным активам были составлены вопросы и ответы, по которым определялась оценка максимального риска.

В соответствии с рисунком 1.5 представлена радарная диаграмма рисков (Kiviat diagram).

В соответствии с рисунком 1.6 представлена дифференциальная диаграмма рисков (Gr.Diff).

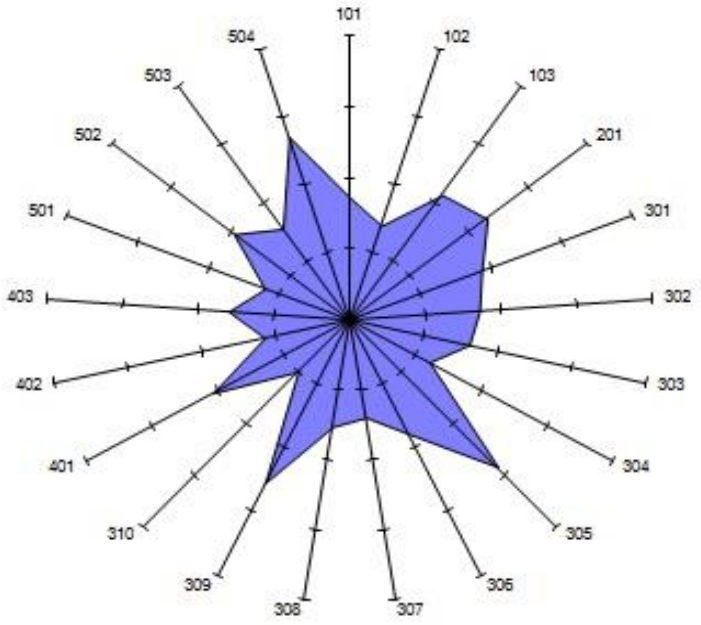

Рисунок 1.5 – Радарная диаграмма рисков (Kiviat diagram)

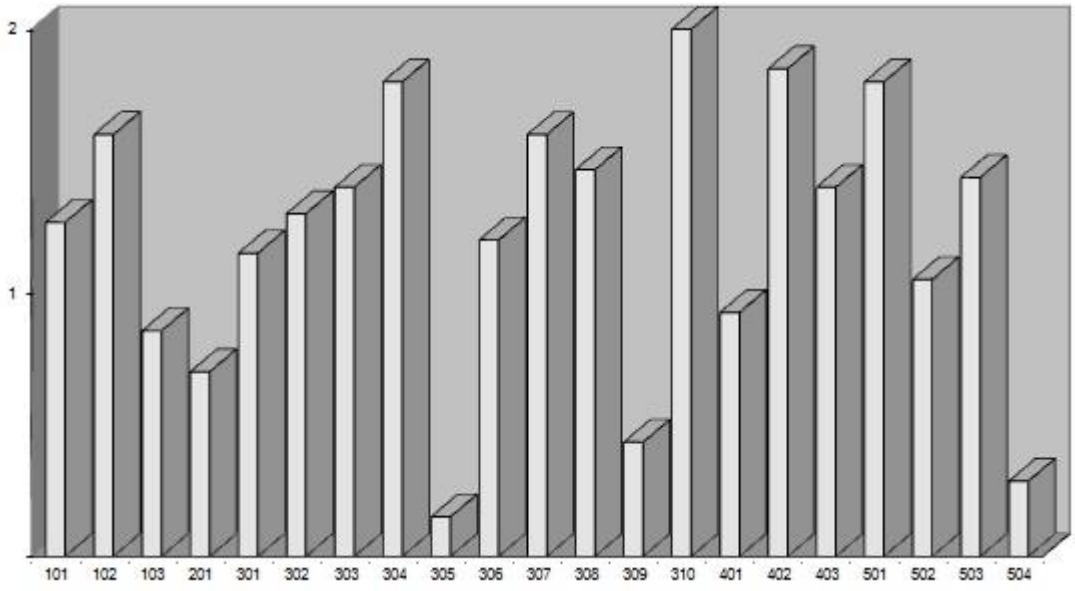

Рисунок 1.6 – Дифференциальная диаграмма рисков (Gr.Diff)

В рамках проведенного анализа можно сделать вывод, что основные активы отделения срочного социального обслуживания имеют низкий уровень защищенности.

Список наиболее уязвимых активов отражен в таблице 1.5.

Таблица 1.5 – Список уязвимых активов

Номер актива	Наименование	Примерные мероприятия
101	Общая организация	Организовать группу информационной безопасности, исследование защищенности, управление рисками
102	Общий контроль	Назначить ответственное лицо за информационную безопасность, определить ответственных за обработку информации и ПДн, определить порядок контроля операторов и качества соблюдения ИБ
301	Окружение	Безопасность компьютерных помещений, защита контролируемой территории
302	Контроль физического доступа	Контроль физического доступа в здание, контроль доступа в кабинеты, контроль доступа в контролируемые зоны
303	Загрязнение	Установка кондиционеров
304	Инструкции по безопасности	Разработать инструкции по компьютерной безопасности, проведение инструктажа, проверок.
306	Безопасность от проникновения воды	Проведение анализа трубопроводных систем водоотведения. Меры по защите от подтопления
307	Правильность установки компьютеров	Обеспечить материальные резервы, запасные части, резервирование компьютеров
308	Связь между пользователями и персоналом ИТ	Организовать группу информационной безопасности, резервное копирование данных
310	Стратегия ИТ	Разработка стратегии ИБ, планирование
402	Безопасность телекоммуникаций	Физическая защита аппаратного обеспечения, безопасность сети, контроль и проверки
403	Безопасность баз данных	Администрирование данных, шифрование данных, журналирование и отслеживание доступа
501	Сохранение и восстановление данных	Процедуры хранения, защита хранилищ, аудит и учет носителей
502	Подготовка и передача данных	Безопасность передачи данных, процедуры проверки подлинности вводимых данных, контроль
503	Резервное копирование	Процедуры резервного копирования, план хранения данных, процедуры восстановления и перезапуска, содействие, контроль, аудит, расследования

Далее необходимо сделать постановку задач но обеспечению информационной безопасности отделения срочного социального обслуживания.

1.5 Постановка задач по обеспечение информационной безопасности отделения срочного социального обслуживания

В отделении срочного социального обслуживания реализуется следующий комплекс организационно-технических мер по защите информации и персональных данных:

1. На АРМ пользователей установлено бесплатное антивирусное программное обеспечение — Avast Free Antivirus.
2. Сотрудники подписали соглашение о неразглашении информации.
3. Сотрудники прошли первичный инструктаж по безопасной работе за компьютером.
4. Сотрудники были ознакомлены под роспись с инструкцией по обработке информации с помощью автоматизированных и не автоматизированных средств обработки.
5. АРМ пользователя имеет учетную запись с персональным паролем, который меняется каждые три месяца.
6. На АРМ сотрудников и на серверах установлено лицензионное программное обеспечение: операционные системы – Microsoft Windows 7, Microsoft Windows Server 2008 R2, Microsoft Windows Server 2016 Standard, офисные приложения – LibreOffice.
7. На АРМ пользователей установлены последние обновления для ПО.
8. В кабинетах установлены пожарные извещатели и датчики движения охранной сигнализации, на окнах установлены жалюзи.

Проанализировав реализуемый комплекс организационно-технических мер по защите информации и персональных данных в отделении срочного социального обслуживания, можно выделить следующие недочеты:

1. Вход в помещение учреждения и кабинеты — свободный.
2. Сотрудники слабо ознакомлены с политикой информационной безопасности.

3. Отсутствует централизованная система контроля за действиями пользователей в сети. Отсутствует система защиты от утечки информации посредством использования внешних устройств и носителей.

4. Отсутствует система ограничения ролей, прав, доступа к ПО у пользователя на АРМ.

5. Отсутствует защищенный канал передачи данных.

6. Отсутствует система защиты файлов от компрометации, повреждения, утери.

7. Персональные данные, карточки, журналы хранятся на рабочих столах, не запирающихся шкафах. Не соблюдается режим «чистого стола».

8. Отсутствует контроль над хранением ключевых носителей.

9. Не установлен пароль на служебном мобильном телефоне.

Из вышеуказанных данных следует вывод:

- персональные данные и информация отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.» не достаточно защищена;
- отсутствует комплексная защита;
- не разработана концепция информационной безопасности;
- не доведена до сотрудников политика информационной безопасности;
- не разработаны инструкции по работе с ПДн;
- журналы ответственных и контролируемые зоны отсутствуют;
- слабое техническое оснащение по ограничению угроз и уменьшению уязвимостей.

В таблице 1.6 отражены результаты планируемых мер по обеспечению информационной безопасности.

Таблица 1.6 – Планируемые меры по обеспечению информационной безопасности

Задача по обеспечению информационной безопасности	Степень исполнения
Обеспечить охрану помещений, с защищаемыми ПДн	Не в полных объемах, отсутствует контроль пропускного режима
Обеспечить защиту информации и сведений, являющихся коммерческой тайной	Не исполняется
Организовать работу по созданию, внедрению организационно-распорядительной документации по защите информации	Не в полных объемах
Предотвратить необоснованный допуск и открытый допуск к информации и персональным данным	Не исполняется
выявить и локализовать возможные каналы утечки информации	Не исполняется
Организовать специальное делопроизводство с возможностью безопасного хранения, шифрования данных.	Не исполняется
Организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты	Не исполняется

В связи с чем, было принято решение о разработке комплекса мер по защите информации отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

Выводы по главе 1

В главе 1 на примере муниципального казенного учреждения «Центр социального обслуживания граждан пожилого возраста и инвалидов» был проведен анализ деятельности учреждения. Приведена информация об организационной структуре, показана структура бизнес-процессов учреждения. Проведена идентификация информации, циркулирующей в отделении, идентификация технического и программного обеспечения отделения срочного социального обслуживания. Проведено исследование текущей системы информационной безопасности, анализ угроз и уязвимостей, анализ и оценка рисков. Проведена постановка основных задач по обеспечению информационной безопасности.

Глава 2 Разработка системы информационной безопасности

2.1 Система информационной безопасности

В рамках выпускной квалификационной работы для успешного построения прочной системы информационной безопасности необходимо реализовать последовательный цикл работ по обеспечению защиты информации и персональных данных отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

Этапы разработки системы информационной безопасности отделения срочного социального обслуживания: аудит, проектирование, внедрение, сопровождение и обслуживание.

Благодаря проведенному аудиту был выявлен список защищаемых объектов документооборота, угроз, уязвимостей и проведен анализ рисков и оценка ущерба.

На этапе проектирования необходимо разработать для отделения:

- Концепцию информационной безопасности.
- Политику информационной безопасности.
- Регламенты, положения, инструкции, журналы, перечни, акты.
- Частную модель угроз безопасности ПДн (на примере используемой ИС).
- Список объектов поставки защиты информации (при возможности протестировать на резервном ПЭВМ).

На этапе внедрения необходимо произвести закупку технических, криптографических, программных средств с их дальнейшим вводом в эксплуатацию. Обучить персонал по работе с новыми средствами защиты информации.

На этапе сопровождения и обслуживания ответственному лицу за информационную безопасность обеспечить непрерывное ведение бизнес-процессов отделения, проведение плановых проверок и устранение

инцидентов.

В соответствии с рисунком 2.1 представлена схема цикла работ по обеспечению системы информационной безопасности отделения срочного социального обслуживания.

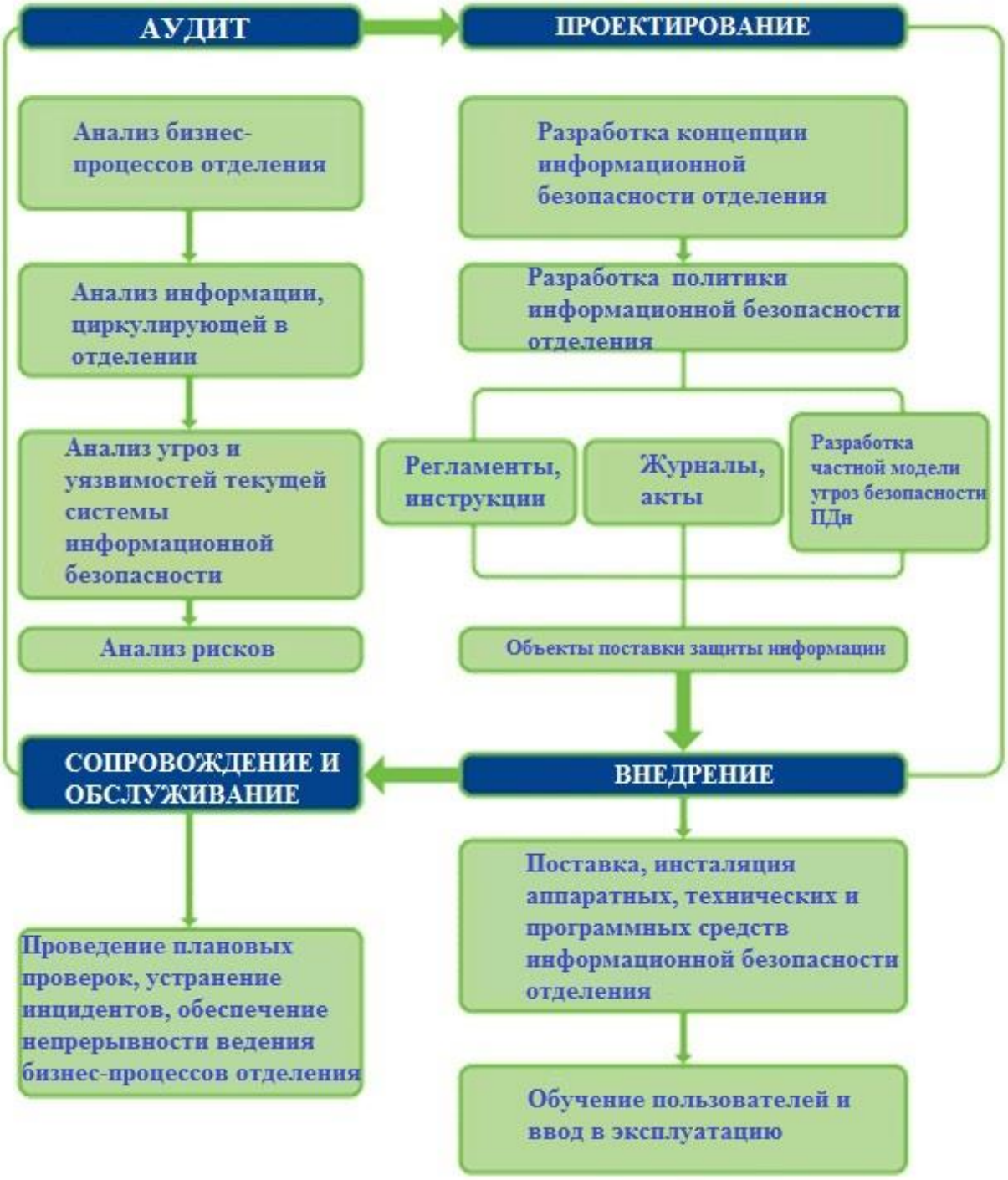

Рисунок 2.1 – Схема цикла работ по обеспечению системы ИБ

Соблюдение цикла работ по обеспечению системы ИБ способствует созданию многоэшелонированной защиты информации и ПДн в отделении срочного социального обслуживания.

В соответствии с рисунком 2.2 представлена контекстная IDEF0-диаграмма организации СЗИ в информационных системах отделения срочного социального обслуживания «КАК ДОЛЖНО БЫТЬ» (0-й уровень).

Рисунок 2.2 – Контекстная IDEF0-диаграмма организации СЗИ в информационных системах «КАК ДОЛЖНО БЫТЬ» (0-й уровень)

2.2 Политика информационной безопасности

Концепция информационной безопасности предназначена для пользователей информационных систем, является документом высокого уровня и необходима для планирования и дальнейшего развития системы защиты информации в МКУ «ЦСОГПВиИ Таштагольского г.п.».

В соответствии с рисунком 2.3 представлена структура концепции ИБ от несанкционированного доступа для отделения срочного социального обслуживания.

Рисунок 2.3 – Структура концепции ИБ

Концепция ИБ создает прочную систему информационной безопасности по таким показателям:

− для нейтрализации актуальных угроз будет применено эффективное техническое, программное или криптографическое средство защиты;

− увеличение рискозащищенности;

− сохранность информации;

− в условиях ограниченного бюджета создается оптимальный комплекс защиты информации и ПДн;

− экономическое обоснование (экономия денежных средств при закупке ПО, лицензий, обновлений и т.п.);

− создание условий для продуктивного использования рабочего времени сотрудниками отделения срочного социального обслуживания.

Концепция информационной безопасности является основой для создания единого распорядительного внутреннего документа в области обеспечения информационной безопасности – политики информационной безопасности.

Политика ИБ необходима для воплощения и управления практических комплексных мер по защите информации и персональных данных в

отделении срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

Для создания многоэшелонированной защиты в отделении необходимо разработать организационно-правовые, физические и программные меры обеспечения безопасности.

В соответствии с рисунком 2.4 представлена схема комплексной системы защиты информации от несанкционированного доступа для отделения срочного социального обслуживания.

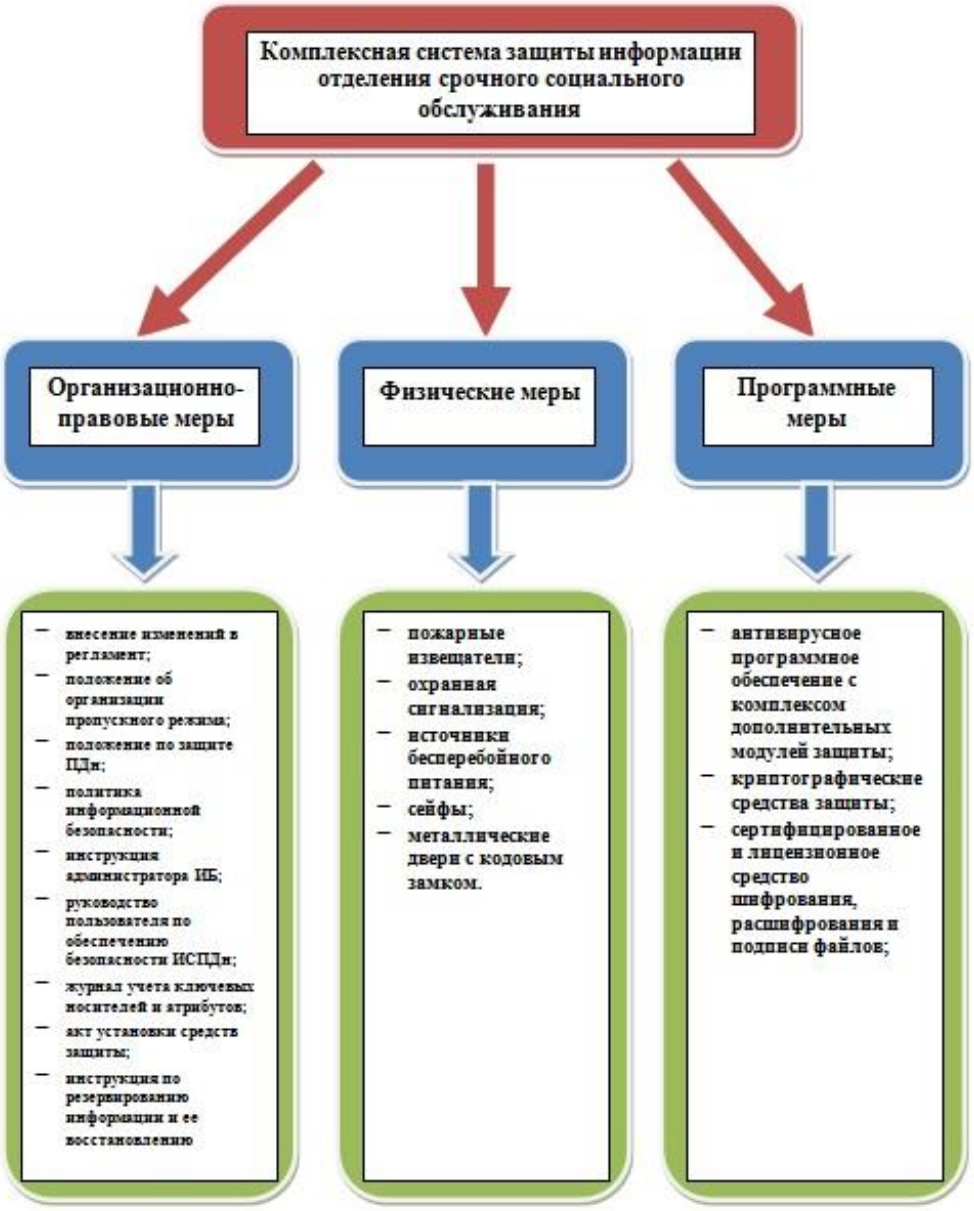

Рисунок 2.4 – Схема комплексной системы защиты информации

Организационно-правовые меры включают распорядительные документы, нормативно-правовые акты, положения, регламенты, инструкции, журналы, руководства.

Физические меры включают охранную и пожарную сигнализацию, и систему ликвидацию угроз.

Программные меры включают в себя программное обеспечение, направленное на снижение угроз, уязвимостей и ограничению доступа к системе информационной безопасности.

2.2.1 Цели и задачи политики ИБ

Политика информационной безопасности отделения срочного социального обслуживания представляет собой систему обеспечения информационной безопасности с перечнем задач и целей защиты информации и персональных данных, а также эффективно выстроенной системой контроля и управления многоэшелонированной защиты информационных систем.

Обеспечение информационной безопасности является приоритетным направлением в деятельности МКУ «ЦСОГПВиИ Таштагольского г.п.».

Цель политики ИБ – защита информационных ресурсов от нанесения вреда, ущерба в результате случайных или преднамеренных действий нарушителей на информацию или ее носители, на процессы обработки и хранения, на процедуры контроля и управления, с целью минимизации рисков ИБ.

Для исполнения поставленной цели необходимо обеспечить эффективное решение поставленных задач [20]:

1. Информация, обрабатываемая в рамках Учреждения, должна быть категорирована, т.е. должен быть составлен перечень ИС Учреждения, в котором должны быть выделены данные (или их группы), содержащие информацию ограниченного доступа.

2. Безопасность информации, отнесенной к информации ограниченного

доступа, обеспечивается в соответствии с требованиями законодательства Российской Федерации.

3. Внутренние документы, определяющие порядок обращения с информацией ограниченного доступа, должны быть разработаны и введены в действие в установленном порядке и содержать способы и методы достижения ИБ.

4. Для обработки информации ограниченного доступа в рамках Учреждения определяется перечень должностей, которым разрешен доступ к такой информации в объеме, необходимом для исполнения должностных обязанностей.

5. Обработка информации ограниченного доступа в рамках Учреждения осуществляется с учетом следующих требований: все работники, использующие документы, содержащие информацию ограниченного доступа, должны быть обеспечены местами для безопасного хранения таких документов, исключающих доступ третьих лиц; помещения, в которых обрабатывается информация ограниченного доступа, должны быть оборудованы охранной сигнализацией. Доступ в указанные помещения может быть ограничен с использованием автоматизированной системы контроля доступа; для управления доступом к информации ограниченного доступа применяются механизмы аутентификации и идентификации; для передачи информации ограниченного доступа могут быть использованы только защищенные каналы связи; защита документов в бумажном и электронном виде осуществляется равноценно.

6. Все используемые в Учреждении ИС, в которых обрабатывается информация ограниченного доступа, должны быть классифицированы, а документы систематизированы и учтены. Для каждой категории информации должен быть определен порядок использования, хранения, передачи, архивации и уничтожения, при котором любой документ можно быстро найти и проконтролировать его использование.

7. Решения, принятые Участниками в отношении ИС, входящих в

Учреждении, должны быть задокументированы, при этом должна обеспечиваться: текущая диагностика сети, вычислительной среды и состояния ресурсов ИС; подотчетность и индивидуальная ответственность действий авторизованных пользователей, осуществляющих доступ; поддержание соответствующего уровня защиты информации в зависимости от категории и области использования информации в Учреждении; контроль и своевременное выявление попыток НСД к защищаемой информации и базам данных Учреждения.

8. Участники должны обеспечить непрерывность деятельности и (или) восстановление деятельности, нарушенной в результате непредвиденных обстоятельств.

9. Все работники, допущенные к обработке информации ограниченного доступа в рамках Учреждения, должны быть ознакомлены под роспись с правилами работы с такой информацией в Учреждении.

10. Участники должны осуществлять мониторинг законодательства Российской Федерации в области защиты информации и принимать меры к совершенствованию способов и средств защиты информации.

Данная политика ИБ распространяется на всех сотрудников отделения срочного социального обслуживания и требует полное исполнение.

2.2.2 Объекты защиты

Основными объектами защиты обеспечения системы информационной безопасности отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.» являются:

− информационные ресурсы, содержащие конфиденциальную информацию;

− информационные ресурсы, содержащие коммерческую тайну;

− информационные ресурсы, содержащие персональные данные;

− открыто распространяемая информация, согласно положению информационной открытости для осуществления деятельности учреждения

по 442-ФЗ;

− информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

Для каждого объекта защиты назначается ответственное лицо согласно приказу руководителя учреждения.

Вся защищаемая информация должна быть классифицирована (проставлены грифы) в соответствии с важностью и степенью доступа.

2.2.3 Организационно-правовые меры обеспечения политики информационной безопасности

В рамках выполнения квалификационной работы для формирования организационно-правовых мер обеспечения политики информационной безопасности необходимо выделить следующие уровни:

− Первый уровень: общий регламент по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR — General Data Protection Regulation)[29]; международные стандарты информационной безопасности ISO17799 ("Нормы и правила при обеспечении безопасности информации")[26]; федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[21]; федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»[22].

− Второй уровень: положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 (далее – Положение)[23]; постановление от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных

данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами (с изменениями на 15 апреля 2019 года)[19].

− Третий уровень: базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.)[24]; методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.)[25].

− Четвертый уровень: политика по обработке персональных данных в МКУ «ЦСОГПВиИ Таштагольского г.п.», руководство пользователя по обеспечению безопасности ИСПДн, инструкция администратора ИБ.

Данные организационно-правовые документы полностью регламентируют обеспечение политики информационной безопасности отделения срочного социального обслуживания.

2.2.4 Аппаратно-программные средства обеспечения политики информационной безопасности

В рамках выпускной квалификационной работы при проведении анализа обеспечения политики информационной безопасности отделения срочного социального обслуживания рассмотрим аппаратно-программные средства на примере информационной системы «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»).

Для начала необходимо соблюсти следующие этапы сбора исходных данных:

а. определение условий создания и использования персональных данных (далее – ПДн), как с использованием средств автоматизированной обработки информации, так и без использования автоматизированной

обработки информации;

б. описание форм представления ПДн;

в. описание структуры;

г. определение характеристик безопасности.

Клиент обращается за оказанием материальной помощи по причине трудной жизненной ситуации. Он пишет письменное заявление в свободной форме на бумажном носителе – его предоставляет на регистрацию специалистам по социальной работе в отделение срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

Заявление регистрируется специалистом по социальной работе в журнале «Регистрация обращений», где указывается причина обращения.

Клиенту выдается бланк-согласия на обработку персональных данных (Приложение А) для заполнения. После получения согласия клиента на обработку его ПДн, специалист по социальной работе приступает к созданию персональной карточки учета на бумажном носителе, проводя опрос клиента на получение дополнительной информации при составлении акта обследования жилищно-бытовых условий (Приложение Б).

Готовую информацию на бумажных носителях заносят в электронное личное дело ИС «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»).

В бланке-согласии на обработку ПДн указывается: цель обработки, состав ПДн, действия, осуществляемые с данными в ходе их обработки, условия прекращения. В журнале «Регистрация обращений» указывается: ФИО, адрес проживания, дата рождения. В карточке учета указывается: ФИО, адрес проживания, дата рождения, состав семьи, условия проживания (жилищно-бытовые условия), информация о предыдущих обращениях.

Информационная система «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP») содержит

персональные данные (паспортные данные, СНИЛС, ИНН, ветеранские, справки, номера телефонов, состав семьи, размер получаемой помощи, признаки учета, индивидуальные программы, перечень социальных услуг и многое другое), отсканированные формы дубликата и оригинала документов клиентов. По видам форм представления ПДн с учетом как с использованием средств автоматизированной обработки информация, так и без использования автоматизированной обработки информации выделим следующие носители:

- Речевая информация.
- Видовая информация (текст, изображения).
- Информация, представленная в виде бит, байт, файлов и других логических структур.

На основе анализа условия создания и использования ПДн выделим структуру элементов информационной системы персональных данных (далее – ИСПДн):

- информация на бумажных носителях хранится в помещении учреждения, может перемещаться сотрудниками из кабинета в кабинет, располагаться как на столах сотрудников, так и в отдельных открытых шкафах (по типу картотеки);
- информация в электронном личном деле хранится на АРМ (автоматизированное рабочее место) пользователя, сервере учреждения.

Информационная система «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP») является клиент-серверной системой, работающей на основе web-технологий. Не требует установки на компьютер пользователя. Работа осуществляется с помощью интернет-браузера. К основным объектам защиты при работе в информационной системе «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP») относятся:

- АРМ пользователей.
- Персональные данные клиентов.
- Серверы.
- Оцифрованная база документов.

Информация на АРМ пользователей обрабатывается и формируется посредством следующего ПО:

1. Офисные приложения (LibreOffice).
2. Операционные системы – Windows 7, Windows 10.
3. Система управления базами данных через программный комплекс «WP».
4. Антивирусное приложение Avast Free Antivirus.

Каналы передачи информации:

- ЛВС (локально-вычислительная сеть).
- Выделенный канал Департамента социальной защиты населения Кемеровской области.
- Переносные устройства хранения – флеш-накопители, мобильные телефоны, фотоаппараты и видеокамеры.

На основе анализа ИСПДн необходимо в информационной системе «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP») обеспечить характеристики безопасности: конфиденциальность, целостность. Конфиденциальность – требование, исключающее передачу информации о клиенте третьим лицам без согласия ее обладателя. Целостность – требование, исключающее искажение, разрушение полученной информации.

В рамках выполнения выпускной квалификационной работы для разработки политики информационной безопасности необходимо составить матрицу доступа – определение пользователей. Согласно политике информационной безопасности учреждения выделим основные группы пользователей информационной системы «Осуществление отдельных

государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»):

− Администратор информационной безопасности (далее – Администратор ИБ).

− Разработчик информационной системы.

− Оператор информационной системы персональных данных. К данной категории относятся сотрудники организации, уполномоченные для выполнения соответствующих ролей.

Согласно политике информационной безопасности учреждения, администратором ИБ назначается приказом директора сотрудник из числа административно-хозяйственной части (АХЧ) в должности системный администратор или инженер-программист. В таблице 2.1 отражена типовая матрица доступа в информационную систему.

Таблица 2.1 – Матрица доступа

Типовая роль	Уровень доступа к ИСПДн	Разрешенные действия
Администратор ИБ	Знание применяемых технических средств и конфигурации системы. Знание установленного системного и прикладного программного обеспечения. Права администратора настройки технических средств и конфигурирования информационной системы.	- сбор; - накопление; - хранение; - систематизация; - уточнение; - использование; - распространение; - обезличивание; - блокирование; - уничтожение.
Разработчик ИС	Обладает информацией об алгоритмах и программах обработки информации. Обладает правами внесения изменений в программное обеспечение. Располагает всей информацией о топологии ИСПДн и технических средств.	- накопление; - хранение; - систематизация; - уточнение; - обезличивание; - блокирование; - уничтожение.
Оператор ИСПДн	Права пользователя для доступа в информационную систему. Знание технических средств для выполнения соответствующих ролей в информационной системе.	- сбор; - накопление; - хранение; - систематизация; - уточнение; - использование; - распространение;

		- обезличивание.

Администратор ИБ согласно должностным инструкциям и инструкции администратора ИБ учреждения обязан обеспечить контроль над выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе, с сохранением конфиденциальности, целостности и доступности информации, а также предотвратить несанкционированное вмешательство третьих лиц. Администратор ИБ составляет список сотрудников для работы в информационной системе согласно нормативному документу учреждения «Перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей». Согласованный директором учреждения список отправляется в Департамент социальной защиты населения Кемеровской области разработчикам ИС – отдел автоматизации и информационных технологий. Разработчики ИС создают для каждого сотрудника из списка персональные идентификационные данные – связка «логин/пароль». Администратор ИБ передает связку «логин/пароль» операторам информационной системы персональных данных для доступа в информационную систему «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»). Прекращение доступа к системе операторам ИСПДн осуществляется в следующих случаях:

− компрометация идентификационных данных (передача связки «логин/пароль» третьему лицу) – нарушение руководства пользователей информационной безопасности учреждения;

− умышленные вредоносные действия по работе с базой данных (искажение, распространение, копирование, уничтожение персональных данных без согласия их обладателя) – нарушение инструкции по обработке персональных данных учреждения;

− кадровое перемещение работника на другую должность или в другое отделение учреждения;

− увольнение работника.

Структура информационной системы «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»):

− распределенная информационная система;

− имеет подключение к сетям международного информационного обмена;

− многопользовательская;

− система с разграничением прав доступа;

− все технические средства находятся на территории РФ.

В таблице 2.2 отражен уровень защищенности информационной системы «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»).

Таблица 2.2 – Уровень защищенности

Технические и эксплуатационные характеристики ИС	Уровень защищенности		
	Высокий	Средний	Низкий
1. По территориальному размещению:			
Распределенная ИС, которая охватывает несколько городов, областей и т.д.	-	-	+
2. По наличию соединения с сетями общего назначения:			
ИС, имеющая одноточечный выход в сеть общего пользования.	-	+	-
3. По встроенным (легальным) операциям с записями баз персональных данных:			
модификация, передача.	-	-	+
4. По разграничению доступа к персональным данным:			
ИС, к которой имеет доступ определенный перечень сотрудников организации, являющейся владельцем ИСПДн, либо субъект ПДн	-	+	-
5. По наличию соединений с другими базами ПДн:			
Интегрированная ИС (организация использует несколько баз ПДн, при этом организация не является владельцем всех используемых баз ПДн).	-	-	+
6.По уровню обезличивания ПДн:			

ИС, в которой предоставляемые пользователю данные не являются обезличенными	-	-	+
7. По объему ПДн, которые предоставляются сторонним пользователям ИС без предварительной обработки:			
ИС, предоставляющая всю базу данных с ПДн	-	-	+

Исходя из данных структуры, информационная система «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP») является распределенной информационной системой II типа – система, имеющая подключение к сетям международного информационного обмена, с разграничением прав доступа.

Фактический уровень защищенности согласно техническим и эксплуатационным характеристикам ИС имеет низкую степень защищенности, т.к. менее 70% характеристик ИС относятся к среднему и высокому уровню.

2.2.5 Модель нарушителя

Угроза информационной безопасности реализуется при образовании канала между несанкционированным источником и носителем информации.

В информационной системе «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP») источниками угрозы являются: нарушитель и носитель вредоносной программы. К нарушителям относятся внешние и внутренние.

Внешние нарушители – клиенты учреждения, случайные посетители.

Внутренние нарушители – пользователи ИСПДн, администраторы баз данных, обслуживающий персонал сторонних организаций.

Предполагается, что нарушители не смогут реализовать средства угрозы безопасности в информационной системе, если в ней нет уязвимостей.

В таблице 2.3 отражена информация о видах нарушителя и их возможной мотивации реализации угроз безопасности информации в отделении срочного социального обслуживания.

Таблица 2.3 – Модель нарушителя и его мотивация

№	Вид нарушителя	Тип нарушителя	Возможная мотивация реализации угроз безопасности информации и ПДн
1	Террористические и экстремистские группировки	Внешний	Идеологические и политические мотивы. Дискредитация и дестабилизация деятельности муниципального учреждения. Нанесение ущерба.
2	Криминальные группировки	Внешний	Мошенничество. Кража данных, с целью получения финансовой выгоды. Дискредитация и дестабилизация деятельности муниципального учреждения.
3	Внешние субъекты (клиенты, случайные посетители)	Внешний	Идеологические и политические мотивы. Мошенничество. Самореализация. Кража данных, с целью получения финансовой выгоды. Дискредитация и дестабилизация деятельности муниципального учреждения.
4	Конкурирующие организации	Внешний	Причинение морального вреда, с целью получения преимущества в рейтинге независимой оценке качества оказываемых услуг
5	Разработчики программно-технических средств	Внешний	Непреднамеренные, неумышленные, низко квалифицированные действия. Причинение ущерба.
6	Обслуживающий персонал сторонних организаций	Внутренний	Причинение имущественного ущерба. Непреднамеренные, неумышленные, низко квалифицированные действия.
7	Администраторы баз данных, администраторы ИС	Внутренний	Причинение имущественного ущерба. Непреднамеренные, неумышленные, неквалифицированные действия.
8	Пользователи ИС	Внутренний	Месть за ранее совершенные действия. Самореализация. Причинение имущественного ущерба. Непреднамеренные, неумышленные, неквалифицированные действия.
9	Бывшие сотрудники	Внешний	Причинение имущественного ущерба. Мошенничество.

	учреждения		Месть за ранее совершенные действия.

Стоит обратить внимание, что внешние и внутренние нарушители могут вступать в сговор для повышения своих возможностей по реализации угроз безопасности информации и персональных данных.

2.2.6 Модель угроз безопасности

Разработка частной модели угроз безопасности проводится в соответствии со следующими основными документами:

− Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [21].

− Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных» [22].

− Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 (далее – Положение) [23].

− Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 15 февраля 2008г.) [24].

− Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Утверждена Заместителем директора ФСТЭК России 14 февраля 2008г.) [25].

Основные этапы методологии формирования модели угроз [30]: проведение анализа персональных данных в информационной системе; определение пользователей – матрица доступа; определение типа системы по защите информации; определение текущего уровня защиты информации; определение перечня угроз, уязвимостей и технических каналов утечки

информации; определение возможного уровня реализации угроз; проведение оценки опасности угроз; определение актуальности угроз.

Угроза информационной безопасности возникает как от случайных условий, так и от несанкционированных факторов, которые могут повлечь нарушение конфиденциальности (распространение, копирование), доступности (блокирование) и целостности (изменение, уничтожение).

Основные элементы ИСПДн:

- помещения, кабинеты, где хранится и обрабатывается информация;
- документация на технические и программные компоненты;
- ключевая и парольная информация;
- вспомогательная оргтехника и технические средства защиты (охранно-пожарная сигнализация и т.п.);
- программные средства;
- технические средства обработки ПДн (каналы передачи, приема и обработки информации);
- персональные данные.

Уязвимость – слабое место в ИС, возникает по причине ошибок проектировщиков и разработчиков программного обеспечения. В информационной системе «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» причинами возникновения уязвимостей являются:

- уязвимость системного и прикладного программного обеспечения;
- неправильная настройка технических средств защиты и антивирусного программного обеспечения;
- несанкционированное использование «левых» программ, которые подгружают систему, нагружают ОЗУ;
- внедрение вирусов, программ-шпионов, плагинов;
- неумышленные действия пользователей ИСПДн;
- сбои аппаратно-технических средств.

В таблице 2.4. отражен перечень возможных угроз безопасности информации в информационной системе «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»), их опасность и реализация.

Таблица 2.4 – Перечень угроз

Угрозы	Вероятность реализации угрозы	Возможность реализации угрозы	Опасность угрозы
1. Угроза от утечки по техническим каналам:			
Угроза утечки видовой информации (текст, изображения и т.п.)	низкая	средняя	средняя
2. Угрозы несанкционированного доступа к информации:			
2.1. Угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИСПДн:			
Кража ПЭВМ	маловероятная	средняя	низкая
Кража носителей информации	низкая	средняя	средняя
Кража ключей и атрибутов доступа	низкая	средняя	средняя
Кражи, модификации, уничтожения информации	низкая	средняя	средняя
Вывод из строя узлов ПЭВМ, каналов связи	низкая	средняя	низкая
Несанкционированное отключение средств защиты	средняя	высокая	средняя
2.2. 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)	низкая	средняя	высокая
Недекларированные возможности системного ПО и ПО для обработки персональных данных	низкая	средняя	средняя
Установка ПО не связанного с исполнением служебных обязанностей	низкая	средняя	средняя
2.3. 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	низкая	средняя	средняя
Непреднамеренная модификация (уничтожение) информации сотрудниками	низкая	средняя	низкая
Непреднамеренное отключение средств защиты	низкая	средняя	низкая
Выход из строя аппаратно-программных средств	низкая	средняя	низкая
Сбой системы электроснабжения	маловероятная	средняя	низкая
Стихийное бедствие	маловероятная	средняя	низкая

Продолжение таблицы 2.4 – Перечень угроз

2.4. Угрозы преднамеренных действий внутренних нарушителей:			
Доступ к информации, модификация, уничтожение лиц не допущенных к ее обработке	низкая	средняя	низкая
Разглашение информации, модификация, уничтожение сотрудниками допущенными к ее обработке	низкая	средняя	средняя
2.5.Угрозы несанкционированного доступа по каналам связи:			
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	низкая	средняя	низкая
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	средняя	средняя
Угрозы выявления паролей по сети	средняя	высокая	средняя
Угрозы навязывание ложного маршрута сети	низкая	средняя	низкая
Угрозы подмены доверенного объекта в сети	низкая	средняя	средняя
Угрозы типа «Отказ в обслуживании»	низкая	средняя	средняя
Угрозы удаленного запуска приложений	средняя	высокая	средняя
Угрозы внедрения по сети вредоносных программ	средняя	высокая	высокая

Под вероятностью реализации угрозы подразумевается вероятность объективных предпосылок для осуществления угрозы: маловероятная, низкая вероятность, средняя вероятность, высокая вероятность.

Опасность угроз – вербальный показатель реализации угроз: низкая, средняя, высокая.

В таблице 2.5. отражены правила отнесения угрозы безопасности к актуальной.

Таблица 2.5 – Правила отнесения угрозы безопасности

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

В таблице Приложения Г отражен перечень актуальных угроз и принятые меры защиты информации в информационной системе [27].

На основе частной модели угроз безопасности персональных данных для информационной системы выделим рекомендуемый комплекс мер защиты информации и персональных данных для политики информационной безопасности:

1. Помещение учреждения должно быть оборудовано пожарной сигнализацией с централизованным выходом на пульт.

2. Помещение учреждение должно быть оборудовано охранной сигнализацией.

3. На входе в учреждение должен быть установлен объект пропускного режима с доступом к экстренной кнопке вызова охраны.

4. Обеспечить «чистый рабочий стол» у специалистов социальной работы.

5. В кабинетах установлены сейфы или шкафы с замками,

опечатанные.

6. Экран монитора в кабинетах располагать во время работы так, чтобы исключалась возможность несанкционированного ознакомления с отображаемой на них информацией посторонними лицами, шторы на оконных проемах должны быть завешаны (жалюзи закрыты).

7. На АРМ пользователей должно быть установлено антивирусное ПО с расширенными настройками и дополнительными модулями защиты (брандмауэр, родительский контроль, удаленное управление, контроль устройств и т.п.).

8. Соблюдать требования парольной политики, устанавливающая обязательную сложность и периодичность смены пароля.

9. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена – Интернет и других.

10. Разработать положение о защите персональных данных.

11. Назначить ответственных за соблюдение защиты персональных данных.

12. Разработать и внедрить инструкцию администратора ИБ, руководство пользователя по обеспечению информационной безопасности, политику обработки персональных данных, журнал учета ключевых носителей и атрибутов, акт установки средств защиты (Приложение В), инструкцию по антивирусной защите.

13. Использовать в работе только сертифицированное и лицензионное программное обеспечение.

14. Обеспечить шифрование данных.

15. Резервное копирование файлов и образов системы (отдельный сервер или рабочая станция, внешний жесткий диск и т.п.).

Организация разграничения прав пользователей на установку стороннего ПО, установку аппаратных средств, подключения мобильных устройств и внешних носителей, установку и настройку элементов ИСПДн и средств защиты.

2.2.7 Объекты поставки защиты информации

В рамках выполнения выпускной квалификационной работы для разработки политики информационной безопасности отделения срочного социального обслуживания необходимо определить объекты поставки защиты согласно рекомендуемым действиям по снижению угрозы безопасности ПДн.

Объекты поставки защиты:

1. Антивирусное ПО.

На автоматизированное рабочее место пользователей необходимо установить сертифицированное и лицензионное антивирусное программное обеспечение отечественного производителя — Dr. Web Security Space 12.0.

Предпочтение данному ПО был отдан по совокупности следующих преимуществ:

− низкая стоимость и наличие бонусной программы — 150 дополнительных дней при продлении лицензии;

− защита в реальном времени данных от несанкционированного доступа;

− комплексное решение защиты от всех видов угроз;

− резервное копирование данных;

− мощный инструмент брандмауэра (межсетевой экран) — не позволяет проникнуть в вашу систему третьим лицам;

− блокирование доступа съемных носителей;

− шифрование отдельных файлов, папок и т. д.;

− родительский контроль;

− блокирование доступа к настройкам ПО с помощью пароля;

− нагрузка на систему ниже по сравнению с подобными антивирусным ПО.

2. СКЗИ – средство криптографической защиты информации.

Разграничение доступа пользователей через создание зашифрованного канала передачи данных[28]. Для этого необходимо установить криптопровайдер Крипто-ПРО CSP 4.0 и выше, а также абонентский пункт безопасности Континент-АП 3.7 и выше. Данное решение внедрено и успешно реализуется в отделе бухгалтерии при работе с программным обеспечением казначейства.

Крипто-ПРО – средство криптографической защиты с использованием смарт-карт или usb-ключей.

Континент-АП – модуль защищенного удаленного доступа с использованием алгоритмов сверхвысокой безопасности со встроенным межсетевым экраном, к системам, содержащим персональные данные.

Внедрение данной системы комплексной защиты информации позволит исключить большинство угроз безопасности в информационных системах.

Принцип работы: в Континент-АП прописывается конфигурация настройки выделенного адреса по примеру: https://192.168.0.118. Вход осуществляются по закрытому ключу и сертификату безопасности, либо электронно-цифровой подписи (далее – ЭЦП). Настройки конфигурации паролятся, смена пароля – каждые три месяца. Таким образом, мы можем ограничить число пользователей при работе с информационными системами. Данные будут шифроваться, и передаваться по защищенному каналу с привязкой к usb-ключам и ЭЦП.

3. Защита файлов на АРМ пользователей.

На автоматизированное рабочее место пользователей необходимо установить сертифицированное и лицензионное программное обеспечение КриптоАРМ – предназначено для шифрования, расшифрования и подписи файлов, папок. Работает с большинством известных криптопровайдеров (Крипто-Про, VipNet).

С помощью данного ПО, любые файлы, набранные и отсканированные в электронный вид – можно централизовано хранить в отдельно выделенном

месте (сервер), шифровать и подписывать ЭЦП, тем самым устранив большинство угроз безопасности в информационных системах.

4. Сейфы и запираемые шкафы.

Для хранения usb-ключей закупить один сейф в кабинет администратора ИБ. Usb-ключи с ЭЦП выдавать под роспись ответственным специалистам для работы в информационных системах с фиксацией в журнале учета ключевых носителей, сдавать под роспись за 15 минут до окончания рабочей смены.

5. В кабинеты отделения срочного социального обслуживания закупить шкафы с запираемыми дверцами для хранения бумажной документации (по 1 шкафу в кабинет). Ручки шкафа оборудовать дополнительным кодовым замком и опечатывать в конце каждой смены. Жалюзи и решетки на окнах, а также железные металлические двери уже установлены в учреждении.

6. Дежурный объект с доступом к экстренной кнопке вызова.

Оборудовать при входе в помещение учреждения дежурный объект согласно графику дежурств среди сотрудников.

7. Охранная и пожарная сигнализация установлены.

Дежурному обеспечить доступ к экстренной кнопке вызова охраны - мобильный телефон с кнопкой вызова Росгвардии.

2.2.8 Контроль эффективности политики информационной безопасности

В рамках выпускной квалификационной работы для осуществления контроля эффективности политики информационной безопасности необходимо выполнять следующие рекомендации:

- Контроль должен осуществляться на периодической основе.
- Разработана и утверждена процедура о происшествиях в области информационной безопасности.
- Разработана и утверждена процедура реагирования на происшествия.

− Разработана и утверждена процедура мониторинга систем, уязвимостей для обнаружения инцидентов ИБ.

− Необходимо создать механизм, позволяющий оценивать масштаб и степень ущерба от угроз ИБ.

− Ознакомление сотрудников с данными процедурами.

− Разработан и утвержден план мероприятий по восстановлению операции, обеспечению требуемого уровня доступности информации после прерывания бизнес-процесса.

− Назначить список ответственных за реализацию системы информационной безопасности.

− Разработать и внедрить контролируемые зоны.

Общий контроль эффективности политики информационной безопасности должен осуществлять руководитель учреждения, либо лицо из числа администраторов информационной безопасности, согласно приказу. Общий контроль осуществляется при проведении контрольно-технических проверок с использованием штатных или специализированных программных средств. Оценка эффективности на предмет соответствия установленным требованиям реализованных мер защиты информации и персональных данных осуществляется при проведении контрольно-технических мероприятий с использованием технических и программных средств контроля.

2.2.9 Календарное планирование

В рамках выполнения выпускной квалификационной работы необходимо составить календарное планирование разработки политики информационной безопасности отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.». В таблице 2.6 отражено календарное планирование.

Таблица 2.6 – Календарное планирование

Наименование работы	Минимальная продолжительность работы, дни	Максимальная продолжительность работы, дни
Приказ о назначении ответственного лица за организацию обработки персональных данных	1	2
Изменение должностной инструкции ответственного лица за организацию обработки персональных данных	1	2
Политика обработки персональных данных	2	4
Политика информационной безопасности	3	6
Приказ о назначении администратора ИБ	1	2
Инструкция по обработке персональных данных, осуществляемых без использования средств автоматизации	1	2
Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн	1	2

Продолжение таблицы 2.6 – Календарное планирование

Перечень лиц, допущенных к обработке ПДн	1	2
Перечень ПДн подлежащих защите	1	2
Положение о разграничении прав доступа к ПДн	1	2
Порядок доступа к помещениям, в которых ведется обработка ПДн	1	2
Положение о пропускном режиме	1	2
Инструкция по антивирусной защите	1	2
Инструкция по резервированию информации и ее восстановлению	1	2
Руководство пользователя по обеспечению безопасности ИСПДн	1	2
Журнал контроля обеспечения информационной безопасности и политики безопасности	1	2
Журнал контроля обеспечения информационной безопасности ИСПДн	1	2
Журнал контроля учета электронных носителей персональных данных	1	2
Журнал регистрации инцидентов при работе системного программного обеспечения	1	2
Журнал учета ключевых СКЗИ	1	2
Журнал учета отклонений от штатного режима работы инфокоммуникационной системы	1	2

Руководство по обеспечению безопасности и средств ЭП	1	2
Акт установки средств защиты информации	1	2
Акт готовности ПЭВМ введения в эксплуатацию	1	2
Разработка частной модели угроз безопасности персональных данных в ИС	1	2
Ознакомление сотрудников с регламентами и нормативно-правовыми актами	2	4
Заключение договоров на поставку ПО, проведение торгов, аукционов	14	28
Проверка технических средств обработки информации	2	3
Составление отчета по результатам анализа	1	2
Составление новых инструкций для пользователей АРМ	2	3
Разделение ролей для АРМ пользователей	2	4
Установка новых средств комплексной защиты информации.	2	3
Составление отчета о дополнительных мерах повышения безопасности	1	2

Продолжение таблицы 2.6 – Календарное планирование

Проведение первичного инструктажа по работе в ИС с внедренными средствами криптографической и программной защиты информации	1	2
Предоставление проекта системы информационной безопасности директору учреждения	1	2
Возможные доработки	1	2
ИТОГО:	57	111

В результате проведенного анализа, делаем вывод, что для реализации политики информационной безопасности отделения срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольскогог.п.» необходимо будет затратить 2-4 месяца. Начало внедрения – II-й квартал 2020 года, окончание внедрения – III-й квартал 2020 года.

2.2.10 Матрица ответственности

В рамках выполнения выпускной квалификационной работы необходимо составить список должностных лиц, участвовавших в разработке

политики информационной безопасности отделения срочного социального обслуживания. В таблице 2.7 отражена матрица ответственности.

Таблица 2.7 – Матрица ответственности

Задачи	Системный администратор	Заведующий отделением	Специалист по социальной работе	Руководители учреждения
Определение состава участников	x			x
Разработка нормативно-правовой документации по системе информационной безопасности	x			
Разработка частной модели угроз безопасности персональных данных в ИС	x			
Ознакомление сотрудников с регламентами и нормативно-правовыми актами	x	x	x	

Продолжение таблицы 2.7 – Матрица ответственности

Предоставление ТЗ на поставку ПО при проведении торгов, аукционов	x			
Проверка технических средств защиты информации	x			
Составление отчета по результатам анализа	x			
Составление новых инструкций для пользователей АРМ	x			
Разделение ролей для АРМ пользователей	x			
Установка новых средств комплексной защиты информации. Проверка.	x			
Составление отчета о дополнительных мерах повышения безопасности	x			
Проведение первичного инструктажа по работе в ИС с внедренными средствами криптографической и программной защиты информации	x	x	x	
Предоставление проекта системы	x			x

информационной безопасности директору учреждения				

В результате проведенного анализа, делаем вывод, что ответственность за соблюдение положений политики ИБ в отделении срочного социального обслуживания должен заниматься квалифицированный специалист в должности системный администратор.

Выводы по главе 2

В данной главе 2 на примере отделения срочного социального обслуживания муниципального казенного учреждения «Центр социального обслуживания граждан пожилого возраста и инвалидов Таштагольского городского поселения» был рассмотрен вопрос разработки политики информационной безопасности.

Представлена схема циклов по обеспечению информационной безопасности в отделении срочного социального обслуживания, структура концепции ИБ, схема комплексной системы защиты информации от несанкционированного доступа. Представлена политика ИБ, определены объекты защиты, определена модель нарушителя, контроль эффективности обеспечения информационной безопасности.

Разработана частная модель угроз безопасности персональных данных на примере информационной системы «Осуществление отдельных государственных полномочий в сфере социальной поддержки и социального обслуживания населения» (программная среда «WP»).

Определен текущий уровень защиты информации, выявлен перечень угроз, уязвимостей, каналов утечки информации. Проведен анализ и оценка актуальности угроз, степень их опасности для системы информационной безопасности.

Предложен рекомендуемый комплекс организационно-технических мер защиты информации и персональных данных по обеспечению

информационной безопасности, который должен предотвратить действия нарушителей и снизить уровень угрозы безопасности.

Определен список поставки защиты информации. Представлено календарное планирование внедрения системы информационной безопасности и отображена матрица ответственности.

В результате предложенных технических и программных средств, модулей безопасности была разработана многоэшелонированная защита обеспечения информационной безопасности в отделении срочного социального обслуживания.

Глава 3 Экономическое обоснование внедрения политики информационной безопасности

Для реализации политики информационной безопасности в рамках системы информационной безопасности отделения срочного социального обслуживания необходимо указать стоимость внедрения объектов поставок защиты. Весь товар приобретается через систему контрактных закупок. В стоимость затрат включена доставка. Все работы по внедрению объектов по защите информации проводятся сотрудниками учреждения своими силами. Дополнительные трудовые затраты не предусмотрены. В таблице 3.1 отражены затраты на приобретение и организацию объектов поставок защиты в отделении срочного социального обслуживания МКУ «ЦСОГПВиИ Таштагольского г.п.».

Таблица 3.1 – Стоимость затрат

Наименование услуги	Количество, шт.	Общая стоимость, руб.
Стоимостные затраты на обработку информации		
Приобретение Dr.web Security Space 12.0 (на 1 год)	5	6 500
Приобретение лицензии Крипто-ПРО 4.0 (бессрочная)	5	6 000
Приобретение лицензии на использование Континент-АП 3.7 (бессрочная)	5	2 500
Приобретение usb-ключей, объемом на 4 GB	5	3 000
Приобретение Крипто-АРМ (бессрочная)	5	6 000
Итого:		24 000
Дополнительные затраты		
Приобретение сейфа	1	3 000
Приобретение шкафа с запирающим кодовым замком	2	22 000
Приобретение мобильного телефона для экстренной кнопки вызова	1	1 500
Оплата услуги экстренной кнопки вызова	1	6 000
Итого:		32 500
Капитальные затраты:		56 500

Внедрение данного проекта считаю экономически целесообразным, т. к. первоначальные затраты в 56 500 руб. рассчитаны на первый год. Затраты на следующий год будут еще меньше, так как уже необходимо будет приобретать только продление лицензий на антивирусное программное обеспечение (6 500 руб.). За невыполнение требований по защите информации предусмотрены: административный штраф на граждан в размере от тридцати тысяч до пятидесяти тысяч рублей; на должностных лиц - от ста тысяч до двухсот тысяч рублей; на юридических лиц - от одного миллиона до шести миллионов рублей. За повторное нарушение штрафы еще выше.

Предположим, что штраф выдан на должностное лицо в размере 100 тыс. руб. – это будут стоимостные затраты на обработку информации по базовому варианту (C_0).

C_1 = 24 000 руб. – это стоимостные затраты на обработку информации по предлагаемому варианту.

Абсолютное снижение стоимостных затрат:

$_{\Delta}C = C_0 - C_1$ = 100 000 – 24 000 = 76 000 руб.

Коэффициент относительного снижения стоимостных затрат $К_с$ (в процентах), определяется по формуле:

$K_c = (_{\Delta}C / C_0) * 100\%$ = (76 000 / 100 000)*100% = 76%

Индекс снижения стоимостных затрат рассчитывается по формуле:

$Y_c = C_0 / C_1$ = 100 000 / 24 000 = 4,17

В таблице 3.2 отражен показатель эффективности от внедрения комплекса мер защиты информации.

Окупаемость затрат ($Т_{ок}$) на приобретение поставок защиты информации в ИС «Регистр получателей социальных услуг» рассчитывается по формуле:

$(T_{ок}) = K_п /_{\Delta}C$,

где $К_п$ – капитальные затраты на создание проекта.

($Т_{ок}$) = 56 500 / 76 000 = 0,74

Таблица 3.2 – Показатель эффективности

Показатель	Затраты		Абсолютное изменение затрат, $_{\Delta}C$	Коэффициент изменения затрат, $К_с$	Индекс изменения затрат, $Y_с$
	Базовый вариант	Проектный вариант			
Стоимость	100 000 руб.	24 000 руб.	76 000 руб.	76%	4,17

Таким образом, капитальные затраты на разработку системы информационной безопасности окупаются менее чем за год (270 дней).

Выводы по главе 3

В данной главе 3 на примере отделения срочного социального обслуживания муниципального казенного учреждения «Центр социального обслуживания граждан пожилого возраста и инвалидов Таштагольского городского поселения» был рассмотрен вопрос экономического обоснования внедрения политики информационной безопасности.

Экономические расчеты показывают эффективность внедрения проекта. Согласно расчетам, окупаемость информационной безопасности произойдет менее чем за год – минимальная финансовая нагрузка для бюджетного учреждения.

Заключение

В рамках выполнения выпускной квалификационной работы была поставлена цель – разработка политики информационной безопасности отделения срочного социального обслуживания (на примере МКУ «ЦСОГПВиИ Таштагольского г.п.»).

В ходе выполнения бакалаврской работы достигнуты следующие результаты:

- Проведен анализ имеющейся системы информационной безопасности.
- Определен текущий уровень защиты информации, выявлен перечень угроз, уязвимостей, каналов утечки информации.
- Проведен анализ и оценка рисков.
- Разработана политика информационной безопасности отделения срочного социального обслуживания (на примере МКУ «ЦСОГПВиИ Таштагольского г.п.»)
- Разработан рекомендуемый комплекс организационно-технических мер по обеспечению системы информационной безопасности, который должен предотвратить действия нарушителей и снизить уровень угрозы безопасности.
- Определен список поставки защиты информации, рассчитана стоимость их внедрения и приведено экономическое обоснование внедрения.

Перспектива дальнейшего развития – разработанная политика информационной безопасности отделения строчного социального обслуживания можно по аналогии внедрить за минимальные затраты во все отделы учреждения – отделения социальной помощи на дому, бухгалтерия, кадры, делопроизводство и другие, используя те же самые объекты поставки защиты. Действия и меры разработанной документации по информационной безопасности распространить на все отделы учреждения.

Список используемой литературы и используемых источников

1. Балдин, К. В. Информационные системы в экономике [Электронный ресурс]: учебник / К. В. Балдин, В. Б. Уткин. – 8-е изд., стер. – Москва: Издательско-торговая корпорация «Дашков и К», 2019. – 394 с. – ISBN 978-5-394-03244-8.

2. Вдовин, В. М. Предметно-ориентированные экономические информационные системы [Электронный ресурс]: учебное пособие / Вдовин В.М., Суркова Л.Е., Шурупов А.А., – 3-е изд. – Москва: «Дашков и К», 2016. – 388 с. – ISBN 978-5-394-02262-3.

3. Золотов С. Ю. Проектирование информационных систем [Электронный ресурс]: учеб. пособие / С. Ю. Золотов ; Томский гос. ун-т систем управления и радиоэлектроники. – Томск: Эль Учебное пособие Контент, 2013. – 86 с. – ISBN 978-5-4332-0083-8.

4. Рыбалова Е. А. Управление проектами [Текст] : учеб. метод. пособие/ Е. А. Рыбалова ; Томский гос. ун-т систем управления и радиоэлектроники. – Томск: ТУСУР, 2015. – 149 с.

5. Елиферов, В.Г. Бизнес-процессы [Электронный ресурс]: регламентация и управление: учебник / В.Г. Елиферов, В.В. Репин. – М.: ИНФРА-М, 2018. – 319 с.

6. Реинжиниринг бизнес-процессов [Электронный ресурс] : учеб. пособие / А. О. Блинов [и др.] ; под ред. А. О. Блинова. – Москва: ЮНИТИ-ДАНА, 2015. - 343 с. – ISBN 978-5-238-01823-2.

7. Силич, В.А. Реинжиниринг бизнес-процессов [Электронный ресурс]: учеб. пособие / В.А. Силич, М.П. Силич. – Томск: ТУСУР, 2014. – 199 с.

8. Федеральный закон от 28 декабря 2013 года № 442-ФЗ «Об основах социального обслуживания граждан В Российской Федерации»: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/page-10/ (Дата обращения:

08.04.2020).

9. Положение о Центре: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/pologenie-o-centre/ (Дата обращения: 15.03.2020).

10. Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п." [Электронный ресурс]: URL: http://tash-cso.ru / (Дата обращения: 01.05.2020).

11. Федеральный закон от 08.05.2010 г. № 83-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с совершенствованием правового положения государственных учреждений» (с изменениями от 27.11.2017г.): [Электронный ресурс] // Официальный сайт компании Консультант-Плюс: URL: http://consultant.ru/document/ cons_doc_LAW_100193/ (Дата обращения: 19.04.2020).

12. Постановление администрации Таштагольского района от 07.12.2010 года № 1028-п «Об утверждении порядка принятия решения о создании, реорганизации, изменении типа и ликвидации муниципальных учреждений Таштагольского района»: [Электронный ресурс] // Официальный сайт системы Гарант: URL: https://base.garant.ru/7570602/ (Дата обращения: 01.05.2020).

13. Устав МКУ «ЦСОГПВиИ Таштагольского г.п.»: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/ page1003/ (Дата обращения: 01.05.2020).

14. Постановление Коллегии Администрации КО от 22.12.2014 № 515 «Об утверждении порядков предоставления социальных услуг на дому, в полустационарной форме социального обслуживания и срочных социальных услуг»: [Электронный ресурс] // Официальный сайт системы Гарант: URL: https://base.garant.ru/7645065/ (Дата обращения: 27.04.2020).

15. Регламент «Методика организации и проведения работы отделения срочного социального обслуживания»: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/ page1002/ (Дата обращения: 22.04.2020).

16. Приказ Министерства труда и социальной защиты Российской Федерации от 28.03.2014 № 159н «Об утверждении форм заявления о предоставлении социальных услуг» »: [Электронный ресурс] // Официальный сайт информационного канала Техэксперт: URL: http://rdocs3.kodeks.ru/document/412801841/ (Дата обращения: 13.04.2020).

17. Положение об отделении срочного социального обслуживания»: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/ page1002/ (Дата обращения: 27.04.2020).

18. Положение о социальном такси: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/ page1002/ (Дата обращения: 22.04.2020).

19. Постановление от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" »: [Электронный ресурс] // Официальный сайт системы Гарант: URL: https://base.garant.ru/70152982/ (Дата обращения: 17.04.2020).

20. Политика информационной безопасности: [Электронный ресурс] // Официальный сайт ОГБУЗ Поликлиника №4: URL: http://xn--4-7sbxaakcdcvfl.xn--p1ai/files/politika_inf_bezopasn.pdf (Дата обращения: 26.05.2020).

21. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации»: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/ page10/ (Дата обращения: 11.04.2020).

22. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»: [Электронный ресурс] // Официальный сайт МКУ "ЦСОГПВиИ Таштагольского г.п.": URL: http://tash-cso.ru/ page10/ (Дата обращения: 01.05.2020).

23. Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденное постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781: [Электронный ресурс] // Официальный сайт системы Гарант: URL: https://base.garant.ru/192223/ (Дата обращения: 01.05.2020).

24. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных: [Электронный ресурс] // Официальный сайт ФСТЭК: URL: https://fstec.ru/component/attachments/download/289/ (Дата обращения: 06.05.2020).

25. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: [Электронный ресурс] // Официальный сайт ФСТЭК: URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380/ (Дата обращения: 08.05.2020).

26. Common Vulnerabilities and Exposures: [Electronic resource]: URL: https://cve.mitre.org/index.html (date of treatment: 04.05.2020).

27. Dark Reading: [Electronic resource]: URL: https://www.darkreading.com/ (date of treatment: 04.05.2020).

28. Alan G. Konheim, Computer Security and Cryptography: [Electronic resource]: Computer security & cryptography / by Alan G. Konheim.p. 542.Includes bibliographical references and index – ISBN-13: 978-0-471-94783-7

29. EUR-Lex Access to European Union Law: [Electronic resource]: URL: https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1531414996493&uri= CELEX:32016R0679/(date of treatment: 05.05.2020).

30. Kord Davis with Doug Patterson, Ethics of Big Data: [Electronic resource]: by Kord Davis with Doug Patterson (O'Reilly). p. 82.Copyright 2012 Kord Davis, – ISBN-978-1-449-31179-7

Приложение А

Бланк-согласие на обработку персональных данных

Я, _____,
(Ф.И.О)
_____ серия _____ № _____ выдан _____
(вид документа, удостоверяющего личность)
_____,
(когда и кем)
проживающий (ая) по адресу :_____
_____,
настоящим даю свое согласие на обработку _____
_____
(наименование и адрес оператора (органа исполнительной власти)

моих персональных данных и подтверждаю, что, давая такое согласие, я действую своей волей и в своих интересах.

Согласие дается мною для целей:
_____
(цель обработки персональных данных)
и распространяется на следующую информацию: _____
_____
_____.
(перечень персональных данных)

Настоящее согласие предоставляется на осуществление любых действий в отношении моих персональных данных, которые необходимы или желаемы для достижения указанных выше целей, включая (без ограничения) сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передача), обезличивание, блокирование, уничтожение, трансграничную передачу персональных данных, а также осуществление любых иных действий с моими персональными данными с учетом федерального законодательства.

В случае неправомерного использования предоставленных мною персональных данных согласие отзывается моим письменным заявлением.

Данное согласие действует с «__» _____ ____ г. по «__» _____ ____ г.

_____
(Ф.И.О., подпись лица, давшего согласие)

Приложение Б

Акт обследования жилищно-бытовых условий

Муниципальное казённое учреждение
«Центр социального обслуживания
граждан пожилого возраста
и инвалидов
Таштагольского городского поселения»
652990, Кемеровская область,
Таштагольский район,
г. Таштагол, ул. Ленина, 64
Тел./факс 3-33-92
e-mail: tash-cson@dsznko.ru
веб-сайт: tash-cso.ru
ОКПО 36686639 , ОГРН 1024201963290
ИНН/КПП 4228005243/422801001

АКТ
обследования жилищно-бытовых условий

от « ___ » _____2020 г. №

Ф. И. О._____
Дата рождения: _____**Паспорт (серия и номер)**_____
Выдан:_____
Адрес регистрации:_____
Адрес фактического проживания:_____
Номер телефона (домашний, сотовый):_____
СНИЛС _____ **ИНН**_____
Социальная категория:_____
Наличие правительственных наград:_____
Наличие льгот:_____
Дата ухода на пенсию, трудовой стаж: _____
Последнее место работы, должность: _____
Среднемесячный доход:_____
Состояние жилья:_____
Квартиросъемщик: _____
Жилой фонд:_____

Сведения о членах семьи, проживающих совместно:

Степень родства	Ф.И.О.	Год рождения	Род занятий	Доход

Продолжение Приложения Б

Акт обследования жилищно-бытовых условий

Сведения о членах семьи, проживающих отдельно:

Степень родства	Ф.И.О.	Год рождения	Род занятий	Доход

Состояние здоровья заявителя:_____
_____
_____

Фактический уровень жизни (наличие предметов первой необходимости, одежды, продуктов питания):_____
_____
_____
_____

Нуждается ли в обслуживании ЦСО (состоит на учёте, вид оказываемых услуг) или другого учреждения:_____
Виды и размеры социально-экономической помощи, оказанной учреждениями социальной защиты населения:_____
_____
_____
_____

Виды и размеры помощи, оказанной из других источников:_____
Вопросы и проблемы, с которыми обратился заявитель:_____
_____

Выводы проверяющих:_____
_____
_____
_____
_____
_____
_____

Выводы комиссии:

Акт составили:

должность	подпись	Ф. И. О.
должность	подпись	Ф. И. О.
должность	подпись	Ф. И. О.

Приложение В

Акт установки средств защиты

Утверждаю

_____

(должность руководителя организации)

_____

(подпись)

«___» _____20___ г.

Акт установки

средств защиты информации
на объекте вычислительной техники - автоматизированное рабочее место
на базе автономной ПЭВМ (инв. №_____)

расположенном в помещении (кабинете) № _____

«___»20___года произведена установка следующих средств защиты информации:

№ п/п	Наименование и тип технического средства	Заводской (серийный) номер	Сведения о сертификате	Место и дата установки
1.				
2.				
3.				

Монтаж средств защиты информации выполнен в соответствии с требованиями технической документации. В ходе инструментальной проверки установлено, что средства защиты информации работоспособны и обеспечивают защищенность информации.

После установки комплекса СЗИ _____ системный блок инв. № _____ опломбирован – пломба №_____.

Ответственный за защиту информации И.О. Фамилия

_____ _____

Дата Подпись

Приложение Г

Перечень актуальных угроз и меры защиты

Таблица Г.1 – Перечень актуальных угроз и меры защиты

Угрозы	Актуальность угрозы	Меры защиты	
		Технические	Организационные
1. Угроза от утечки по техническим каналам:			
Угроза утечки видовой информации (текст, изображения и т.п.)	Актуальная	расположение экрана монитора АРМ пользователя; жалюзи на окна.	Пропускной режим
			Руководство пользователя по информационной безопасности
2. Угрозы несанкционированного доступа к информации:			
2.1. Угрозы уничтожения, хищения аппаратных средств ИС носителей информации путем физического доступа к элементам ИСПДн:			
Кража ПЭВМ	Неактуальная	Охранная сигнализация	Пропускной режим
		Решетки на окна	Дежурный на входе в помещение. Доступ к экстренной кнопке вызова Росгвардии.
		Металлическая дверь с кодовым замком	Акт установки средств защиты
		Шифрование данных	
Кража носителей информации	Актуальная	Охранная сигнализация	Акт установки средств защиты
		Хранение в сейфе или запираемом шкафе с опечатыванием	Учет носителей информации
		Шифрование данных	
Кража ключей и атрибутов доступа	Актуальная	Хранение в сейфе или запираемом шкафе с опечатыванием	Учет носителей информации
			Руководство пользователя при работе с ключевыми носителями
Кражи, модификации, уничтожения информации	Актуальная	Охранная сигнализация	Акт установки средств защиты
		Решетки на окна	
		Металлическая дверь с кодовым замком	
		Шифрование данных	
		Система защиты от НСД	

Продолжение таблицы Г.1

Вывод из строя узлов ПЭВМ, каналов связи	Неактуальная	Охранная сигнализация	Пропускной режим
		Решетки на окна	Дежурный на входе в помещение.
		Металлическая дверь с кодовым замком	
Несанкционированное отключение средств защиты	Актуальная	Настройка средств защиты, защищенная паролем	Инструкция администратора ИБ
			Технологический процесс обработки
			Руководство пользователя по информационной безопасности
			Акт установки средств защиты
2.2. 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)	Актуальная	Антивирусное ПО с расширенными настройками и дополнительными модулями защиты (брандмауэр, родительский контроль, удаленное управление, контроль устройств и т.п.)	Руководство пользователя по информационной безопасности
			Инструкция по антивирусной защите
			Инструкция администратора ИБ
Недекларированные возможности системного ПО и ПО для обработки ПД	Актуальная	Лицензионное программное обеспечение, рекомендованное ФСТЭК	Сертифицированное ПО
Установка ПО не связанного с исполнением служебных обязанностей	Актуальная	Настройка средств защиты	Руководство пользователя по информационной безопасности
2.3. 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	Хранение в сейфе или запираемом шкафе с опечатыванием	Руководство пользователя по информационной безопасности
			Инструкция администратора ИБ

Продолжение таблицы Г.1

Непреднамеренная модификация (уничтожение) информации сотрудниками	Неактуальная	Настройка средств защиты	Создание резервных копий на источнике хранения данных (отдельный сервер или рабочая станция, внешний жесткий диск и т.п.)
Непреднамеренное отключение средств защиты	неактуальная	Доступ только у администратора ИБ	Руководство пользователя по информационной безопасности
			Инструкция администратора ИБ
Выход из строя аппаратно-программных средств	Неактуальная	Календарное планирование по комплексному обслуживанию.	Создание образов системы и обеспечить наличие резервной АРМ
Сбой системы электроснабжения	Неактуальная	Использование ИБП	Создание резервных копий на источнике хранения данных (отдельный сервер или рабочая станция).
Стихийное бедствие	Неактуальная	Пожарная сигнализация с централизованным выходом на пульт	Инструкция по охране труда. Памятка о порядке действий при чрезвычайных ситуациях. Ежеквартальные учения.
2.4. Угрозы преднамеренных действий внутренних нарушителей:			
Доступ к информации, модификация и ее уничтожение, лицами, не допущенными к ее обработке	Неактуальная	Система защиты от НСД	Акт установки средств защиты
			Технологический процесс обработки
Разглашение информации, модификация и ее уничтожение, сотрудниками, допущенными к	Актуальная	Система защиты от НСД	Договор о неразглашении
			Руководство пользователя по информационной безопасности

ее обработке			Политика обработки персональных данных

Продолжение Приложение Г

Продолжение таблицы Г.1

2.5.Угрозы несанкционированного доступа по каналам связи:			
Угроза «Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации	Неактуальная	Шифрование данных	Технологический процесс обработки
		Межсетевой экран	Руководство пользователя по информационной безопасности
		Антивирусное ПО с расширенными настройками и дополнительными модулями защиты	Инструкция администратора ИБ
			Акт установки средств защиты
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.	Актуальная	Шифрование данных	Технологический процесс обработки
		Межсетевой экран	Руководство пользователя по информационной безопасности
		Антивирусное ПО с расширенными настройками и дополнительными модулями защиты	Инструкция администратора ИБ
			Акт установки средств защиты
Угрозы выявления паролей по сети	Актуальная	Межсетевой экран	Технологический процесс обработки
		Антивирусное ПО с расширенными настройками и дополнительными модулями защиты	Руководство пользователя по информационной безопасности
			Инструкция администратора ИБ
			Акт установки средств защиты
Угрозы навязывание ложного маршрута сети	Неактуальная	Межсетевой экран	Технологический процесс обработки

Продолжение таблицы Г.1

		Антивирусное ПО с расширенными настройками и дополнительными модулями защиты	Руководство пользователя по информационной безопасности
			Инструкция администратора ИБ
			Акт установки средств защиты
Угрозы удаленного запуска приложений	Актуальная	Межсетевой экран	Технологический процесс обработки
		Антивирусное ПО с расширенными настройками и дополнительными модулями защиты	Руководство пользователя по информационной безопасности
			Инструкция администратора ИБ
			Акт установки средств защиты
Угрозы внедрения по сети вредоносных программ	Актуальная	Межсетевой экран	Технологический процесс обработки
		Антивирусное ПО с расширенными настройками и дополнительными модулями защиты	Руководство пользователя по информационной безопасности
			Инструкция администратора ИБ
			Акт установки средств защиты