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

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

ДОПУСТИТЬ К ЗАЩИТЕ
Зав. кафедрой
_____ А.В. Бушманов
«_____»_____ 2021 г.

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка и внедрение информационной системы с локальным чатом для сотрудников

Исполнитель студент группы 755-об	_____ (подпись, дата)	Д.В. Бурдуковский
Руководитель доцент	_____ (подпись, дата)	И.М. Акилова
Консультант по части безопасности и экологичности, доцент, к.т.н	_____ (подпись, дата)	А.Б. Булгаков
Нормоконтроль доцент, к.т.н	_____ (подпись, дата)	О.В. Жилиндина

Благовещенск 2021

Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего профессионального образования
АМУРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
(ФГБОУ ВО «АмГУ»)
Факультет математики и информатики
Кафедра информационных и управляющих систем

УТВЕРЖДАЮ
Зав. кафедрой
_____ А.В. Бушманов
«____» _____

З А Д А Н И Е

К выпускной квалификационной работе студента Бурдуковского Данила Витальевича.

1. Тема дипломной работы: Разработка и внедрение информационной системы с локальным чатом для сотрудников.
(утверждена приказом 23.04.2021 №812-уч)

2. Срок сдачи студентом законченной работы: 24.06.2021 г.

3. Исходные данные к выпускной квалификационной работе: отчет о прохождении преддипломной практики, нормативная документация, специальная литература.

4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов): анализ предметной области и организации, обоснование необходимости разработки и определение требований, проектирование локально вычислительной сети и программного продукта, оценка надежности и качества функционирования объекта проектирования, описание информационной безопасности системы, обоснование безопасности и экологичности.

5. Консультанты по выпускной квалификационной работе:
по безопасности и экологичности – Булгаков А.Б., доцент, кандидат технических наук.

6. Дата выдачи задания: 20.02.2021 г.

Руководитель выпускной квалификационной работы: Акилова И.М. доцент.

Задание принял к исполнению: 20.02.2021 г._____Бурдуковский Д.В.

РЕФЕРАТ

Отчет содержит 145 с., 8 рисунков, 6 таблиц, 23 источников, 3 приложения.

АНАЛИЗ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ, ПРОЕКТИРОВАНИЕ ИС, БЕЗОПАСНОСТЬ ИС.

В работе выполнено проектирование информационной системы (ИС) с чатом для сотрудников предприятия «ГАУ ДПО «АмИРО» Региональный модельный центр».

Цель работы – проектирование ИС с чатом для сотрудников «ГАУ ДПО «АмИРО» Региональный модельный центр».

Объект исследования – «ГАУ ДПО «АмИРО» Региональный модельный центр».

Результатом работы является разработка и внедрение ИС с чатом для сотрудников.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ

АРМ	Автоматизированное рабочее место
ВТСС	Вспомогательные технические средства и системы
ЗП	Закладное устройство
ЗИ	Защита информации
ИБ	Информационная безопасность
ИС	Информационная система
ИСПДн	Информационная система персональных данных
КЗ	Контролируемая зона
ЛВС	Локальная вычислительная сеть
НСД	Несанкционированный доступ
НПА	Нормативные правовые акты
ОС	Операционная система
ОТСС	Основные технические средства и системы
ПДн	Персональные данные
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
СВТ	Средства вычислительной техники
СУБД	Система управления базами данных
ТС	Техническое средство

ТЗИ	Техническая защита информации
ТКУИ	Технические каналы утечки информации
УБ	Угрозы безопасности
УБПДн	Угрозы безопасности персональных данных
ФЗ	Федеральный закон
ФК	Функциональный компонент
ФСБ России	Федеральная служба безопасности России
ФСТЭК России	Федеральная служба по техническому и экспортному контролю России
ЦОД	Центр обработки данных
ПМВ	Программно-математическое воздействие
ПС	Программное средство
СЗИ	Средства защиты информации
СЗПДн	Система защиты персональных данных
СКЗИ	Средства криптографической защиты информации
СМИ	Средства массовой информации
СФК	Среда функционирования СКЗИ (криптосредства)
РМЦ	«Амурский институт развития образования «Региональный модельный центр»»

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Автоматизированная обработка персональных данных – обработка персональных данных с помощью средств вычислительной техники.

Атака – целенаправленные действия нарушителя с использованием технических и (или) программных средств с целью нарушения заданных характеристик безопасности защищаемой информации или с целью создания условий для этого.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Актуальные угрозы безопасности персональных данных – совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Безопасность информации – состояние защищённости информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения, информации, в том числе её передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты

компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Встраивание СКЗИ – процесс подключения СКЗИ к техническим и программным средствам, совместно с которыми предполагается его штатное функционирование, за исключением процесса инсталляции.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Доступность информации – состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие право доступа, могут реализовывать их беспрепятственно.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Информация - сведения (сообщения, данные) независимо от формы их представления.

Использование персональных данных - действия (операции) с персональными данными, совершаемые должностным лицом организации в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъектов либо иным образом затрагивающих их права и свободы или права и свободы других лиц;

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

Источник угрозы безопасности информации - субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – это пространство, в котором исключено неконтролируемое пребывание сотрудников и посетителей оператора и посторонних транспортных, технических и иных материальных средств. Границей контролируемой зоны может быть: периметр охраняемой территории предприятия (учреждения), ограждающие конструкции охраняемого здания, охраняемой части здания, выделенного помещения.

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя или наличия иного законного основания.

Компьютерная стеганография – скрытная передача информации путём сохранения в тайне самого факта передачи.

Локальная информационная система – комплекс автоматизированных рабочих мест, объединенных в единую информационную систему средствами связи без использования технологии удаленного доступа.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Несанкционированный доступ (несанкционированные действия) –доступ к информации или действия с информацией, осуществляемые с нарушением установленных прав и (или) правил доступа к информации или действий с ней с применением штатных средств информационной системы или средств, аналогичных им по своему функциональному предназначению и техническим характеристикам.

Общедоступные персональные данные - персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Обезличивание персональных данных – действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Оператор – государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а

также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Распространение персональных данных - действия, направленные на передачу персональных данных субъектов определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных субъектов в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным лиц каким-либо иным способом;

Средства криптографической защиты информации – аппаратные, программные и программно-аппаратные средства, системы и комплексы, реали-

зующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации.

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

Угрозы 1-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа – угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа – угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

ВВЕДЕНИЕ

В данной работе будет представлена разработка информационной системы (ИС) с чатом для сотрудников «ГАУ ДПО «АмИРО» Региональный модельный центр». (РМЦ).

В современном мире совершенно очевидно, что автоматизация процессов в организациях является необходимой, так как это значительно ускоряет процесс работы.

«Региональный модельный центр» создавался как абсолютно новое подведомственное подразделения ГАУ ДПО «АмИРО» из чего следует, что есть необходимость создать с нуля информационную систему, включающую в себя локально-вычислительную сеть и локальный чат для сотрудников.

В настоящее время практически у всех организаций есть потребность в возможности обмениваться мгновенными сообщениями. Сейчас, в большинстве случаев это происходит по средствам общеизвестных мессенджеров, таких как WhatsApp или Telegram. Безусловно, эти приложения достаточно удобны для этих целей, но, с точки зрения безопасности, не совсем корректно использовать их в качестве рабочих чатов, так как достоверно не известно где территориально находятся сервера этих приложений, на которых идет обработка информации.

Так же зачастую в этих приложениях становиться слишком много сообщений и становится легко пропустить, например, важные сообщения от работодателя.

Проблема исследования – создание информационной системы с удобной и безопасной среды для обмена мгновенными сообщениями между сотрудниками.

Цель исследования – разработать и внедрить локально-вычилительную сеть с интерфейсными и функциональными модулями локального чата для сотрудников «РМЦ».

Для реализации поставленной цели необходимо решить следующие задачи:

1) Проанализировать предметную область;

2) Рассмотреть структуру организации;

3) Выявить проблемы, которые необходимо устранить с помощью разрабатываемой ИС;

4) Разработать ЛВС и программный модуль локального чата.

Разработать проект, учитывая все требования.

Объектом исследования в данной курсовой работе является организация, которая оказывает поддержку внедрения национального проекта по финансированию дополнительного образования детей «Навигатор дополнительного образования».

Предметом исследования является проектирование и разработка ИС с локальным чатом для сотрудников.

Актуальность проектирования и разработки локального чата заключается в следующем:

– необходимость в автоматизации процессов в организации;

– удобный обмен мгновенными сообщениями между сотрудниками, что необходимо из-за их рассосредоточенности внутри здания;

– безопасность общения, так как все сообщения хранятся только в локальной сети и не доступны из вне;

1 АНАЛИЗ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

«РМЦ» является подведомственной организацией «ГАУ ДПО «Амурский институт развития образования» и занимается внедрением и поддержкой жизнедеятельности национального проекта финансирования дополнительного образования детей «Навигатор дополнительного образования» в Амурской области.

Так же в каждом муниципалитете Амурской области есть муниципальные опорные центры, которые, в свою очередь, подчиняются «Региональному модельному центру» и оказывают поддержку проекта в своих районах.

1.1 Цели и задачи организации

Целью деятельности данной организации является непосредственно поддержка проекта в Амурской области, что подразумевает:

- работу с ИС «Навигатор» и её администрирование;
- поддержку МОЦов;
- распространение информации о «Навигаторе»;
- обеспечение техподдержки для родителей (пользователей ИС «Навигатор»).

Достижение этих целей «РМЦ» обеспечивается выполнением следующих задач:

a) постоянным повышением квалификации администраторов «Навигатора»;

b) нахождением в бесперебойном контакте с МОЦами;

c) работой отдела по связи с общественностью;

d) ежедневным мониторингом почты с обращениями родителей.

1.2 Организационная структура предприятия

Организационная структура предприятия указана на следующем рисунке:

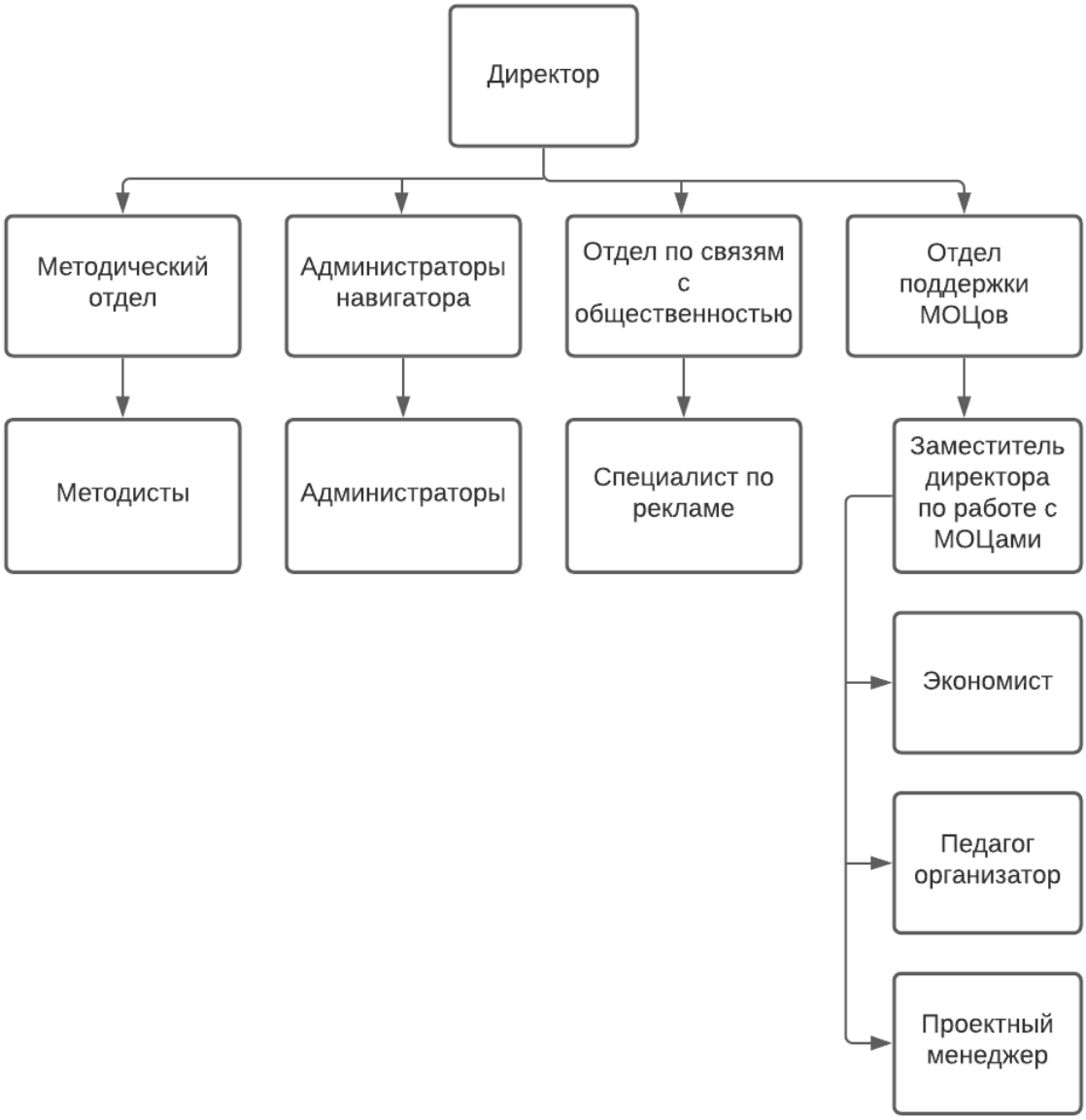

Рисунок 1 – Организационная структура предприятия

Во главе предприятия стоит директор, который осуществляет контроль за предприятием. Директору подчиняются методический отдел, администраторы «Навигатора», отдел по связям с общественностью и отдел поддержки МОЦов. Во главе методического отдела стоит заместитель директора по методической части. Замдиректору подчиняются методисты. В отделе администраторов находятся администраторы ИС «Навигатор». В отделе по связям с общественностью состоит специалист по рекламе и распространению информации. Во главе поддержки МОЦов стоит заместитель директора по работе с

МОЦами и ему подчиняются: экономист, педагог организатор и проектный менеджер.

1.3 Документооборот предприятия

Внешний документооборот – это движение документов в правовом пространстве, в котором действуют и реализуют правоотношения различные субъекты права – физические и юридические лица, граждане, предприятия и организации, органы местного самоуправления, органы государственной власти как между однородными по виду субъектами, так и с другими их видами.

Диаграмма внешнего документооборота представляет собой контекстную диаграмму, построенную в нотации DFD (рисунок 2).

DFD – это методология графического структурного анализа, описывающая внешние по отношению к системе источники и адресаты данных, логические функции, потоки данных и хранилища данных, к которым осуществляется доступ.

Диаграмма потоков данных это один из основных инструментов структурного анализа и проектирования информационных систем.

Модель DFD, как и большинство других структурных моделей — иерархическая модель. Каждый процесс может быть подвергнут декомпозиции, то есть разбиению на структурные составляющие, отношения между которыми в той же нотации могут быть показаны на отдельной диаграмме. Нотация DFD — удобное средство для формирования контекстной диаграммы, то есть диаграммы, показывающей разрабатываемую архитектуру информационной системы в коммуникации с внешней средой. Это — диаграмма верхнего уровня в иерархии диаграмм DFD. Её назначение — ограничить рамки системы, определить, где заканчивается разрабатываемая система и начинается среда.

В ее состав входят один процесс, название которого совпадает с названием предприятия, внешние сущности – субъекты права и потоки документов, которые обеспечивают взаимодействие процесса с внешними сущностями.

Внешний документооборот представлен на рисунке:

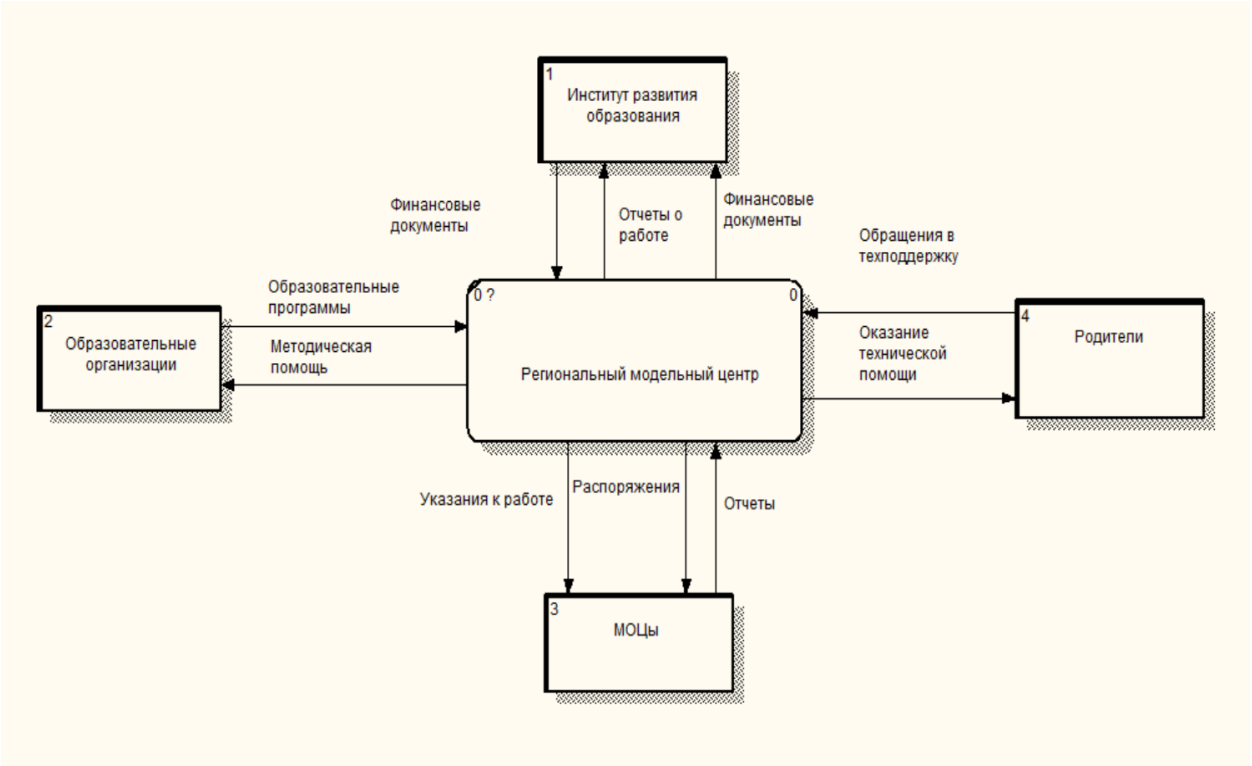

Рисунок 2 – внешний документооборот

Любая DFD-диаграмма может содержать работы, внешние сущности, стрелки (потоки данных) и хранилища данных.

Работы изображаются прямоугольниками с закругленными углами (смысл их совпадает со смыслом работ IDEF0 и IDEF3). Так же как работы IDEF3, они имеют входы и выходы, но не поддерживают управления и механизмы, как IDEF0. Все стороны работы равнозначны. В каждую работу может входить и выходить по несколько стрелок.

Внешние сущности изображают входы в систему и/или выходы из нее. Одна внешняя сущность может одновременно предоставлять входы (функционируя как поставщик) и принимать выходы (функционируя как получатель). Внешняя сущность представляет собой материальный объект, например: заказчики, персонал, поставщики, клиенты, склад. Определение некоторого объекта или системы в качестве внешней сущности указывает на то, что они находятся за пределами границ анализируемой системы. Внешние сущности изображаются в виде прямоугольника с тенью.

Стрелки описывают движение объектов из одной части системы в другую (отсюда следует, что диаграмма DFD не может иметь граничных стрелок). Поскольку все стороны работы в DFD равнозначны, стрелки могут начинаться и заканчиваться на любой стороне прямоугольника. Стрелки могут быть двунаправленные.

Глядя на диаграмму внешнего документооборота, можно сделать вывод о том, что «РМЦ» связано с несколькими внешними сущностями:

1) Образовательные организации;

2) Институт развития образования;

3) Родители;

4) МОЦы;

К сущности Образовательные организации идет одна стрелка – методическая помощь. От сущности Образовательные организации исходят образовательные программы.

От сущности Институт развития образования исходят управляющие документы. К сущности Институт развития образования идут отчеты о работе и финансовые документы.

От сущности Родители приходят обращения в техническую поддержку. К сущности Родители идет оказание помощи.

От сущности МОЦы к «РМЦ» идут отчеты. К сущности МОЦы от «РМЦ» идут распоряжения и указания к работе.

Далее будет рассмотрен внутренний документооборот предприятия «Региональный модельный центр».

Внутренний документооборот – это движение документов внутри предприятия или организации, которые регулируются ведомственными или корпоративными нормативными правовыми актами. Диаграмма также строится в нотации DFD (рисунок 3). При описании внутреннего документооборота представить основные функции каждого подразделения и рабочего места, охарактеризовать хранилища данных и основные документы, циркулирующие внутри предприятия.

Для построения диаграммы внутреннего документооборота необходимо декомпозировать контекстную диаграмму, т.е. диаграмму внешнего документооборота.

Достаточно большой пласт централизованного документооборота составляют так называемые внутренние документы. В их число входят (ОРД), предназначенные для использования только внутри организации. Это могут быть приказы руководства касательно внутренней деятельности организации, протоколы совещаний, различные нормативные документы (должностные инструкции, положения о структурных подразделениях и т. п.).

Утверждение документов проводится должностным лицом (руководителем) соответствующего подразделения или руководителем предприятия, или специально издаваемым документом для придания документу юридической силы. В утвержденных документах присутствует гриф утверждения документа, содержащий слово УТВЕРЖДАЮ, наименование должности, подпись инициалы и фамилию лица, утверждающего документ, и дата утверждения.

На документах, удостоверяющих права должностных лиц, фиксирующих факт расходования денежных средств и материальных ценностей, а также специально предусмотренных правовыми актами ставятся печать и подпись. Подпись должна быть заверена печатью предприятия.

Оттиск печати следует проставлять таким образом, чтобы он захватывал часть личной подписи должностного лица, подписавшего документ, и текст был разборчивым.

Внутренний документооборот:

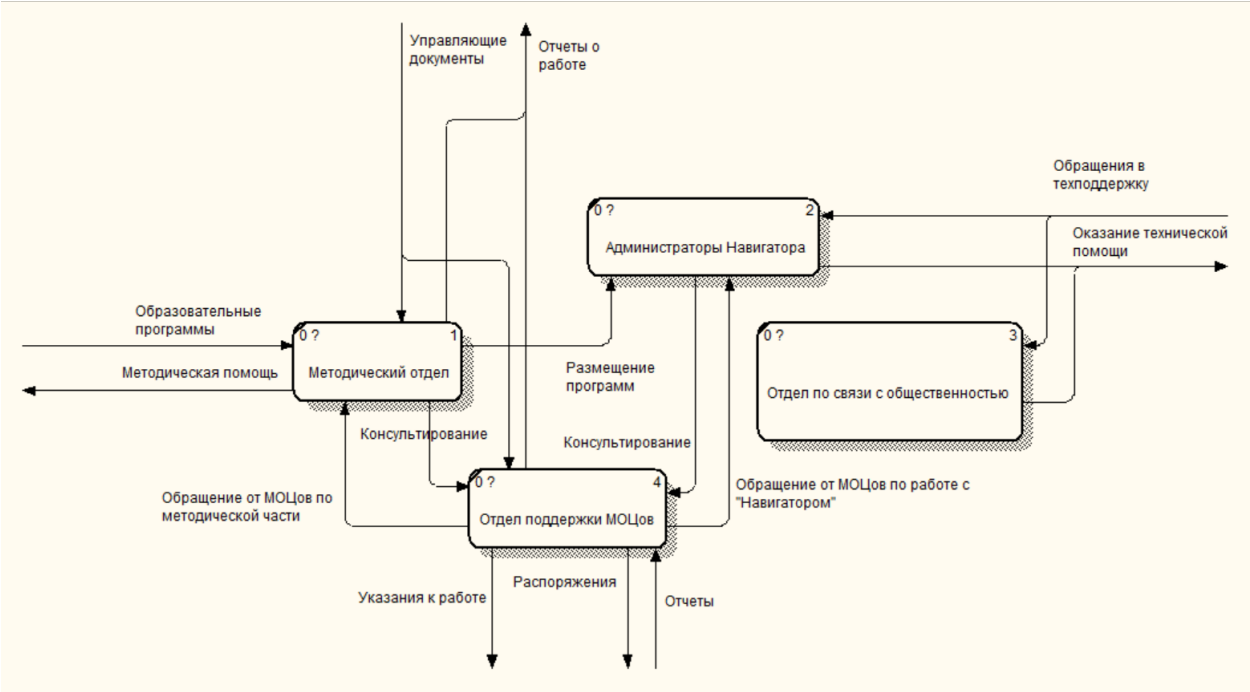

Рисунок 3 – Внутренний документооборот

Имеется четыре отдела, которые работают с документацией.

Первый отдел – методический. К ней идет две стрелки – управляющие документы и образовательные программы. От методического отдела идут методическая помощь и отчеты о работе.

От методического отдела к отделу поддержки МОЦов и к администраторам «Навигатора» идут консультирование и размещение программ, соответственно.

К отделу поддержки МОЦов приходит стрелка отчеты. А от него идут обращения МОЦов по методической части к методическому отделу, обращения МОЦов по работе с «Навигатором» к администраторам «Навигатора» и отчеты о работе.

К администраторам «Навигатора» приходит обращения в техподдержку, от них идут консультирование к отделу поддержки МОЦов и оказание помощи.

К отделу по связи с общественностью приходит обращения в техподдержку и уходит оказание помощи.

2 ПРОЕКТИРОВАНИЕ И ВНЕДРЕНИЕ ЛОКАЛЬНО-ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

2.1 Выбор конфигурации вычислительной сети

Рассмотрим различные варианты конфигурации ЛВС

2.1.1 Выбор типа ЛВС

ЛВС будет обслуживать 13 постоянных пользователей, а также необходимо организовать гостевой доступ. В сети планируется использовать ресурсы и данные, доступ к которым следует контролировать. Возможность распределять сетевые ресурсы и управлять политикой безопасности в сети будет предоставлена системному администратору. В ЛВС планируется применять расширенную защиту, в связи с тем, что информация предприятия накапливается длительное время, она должна быть защищена от несанкционированного редактирования, уничтожения и др. Пользователи сети также должны иметь доступ в интернет. Из приведенных аргументов следует, что необходимо выбрать сеть на основе сервера.

Определим необходимость разрабатываемой сети в серверах. Серверы – это высокопроизводительные компьютеры с винчестерами большой емкости и с высокоскоростной сетевой картой, которые отвечают за хранение данных, организацию доступа к этим данным и передачу данных рабочим станциям или клиентам.

В зависимости от способов использования сервера различают серверы следующих типов:

а) сервер приложений, в этом случае на сервере находятся совместно используемые программы;

б) сервер баз данных, на сервере размещается сетевая база данных;

в) почтовый сервер, на сервере хранится информация, отправляемая и получаемая как по локальной сети, так и по Интернету;

г) факс-серверы – управляют потоком входящих и исходящих факсимильных сообщений через один или несколько факс-модемов;

д) коммуникационные серверы – управляют потоком данных и почтовых сообщений между данной ЛВС и другими сетями или удаленными пользователями через модем и телефонную линию. Они же обеспечивают доступ к Интернету;

е) сервер служб каталогов - предназначен для поиска, хранения и защиты информации в сети.

В соответствии с решаемыми задачами и в связи с выставляемыми высокими требованиями к скорости решения задач и к защите информации, предлагается использовать один высокопроизводительный файловый сервер, на котором находятся совместно-используемые программы и файлы данных. В системе предполагается размещение сетевых принтеров для организации печати.

Сервер будет располагаться централизовано, так как организация располагается на одном этаже трехэтажного здания с выделенной комнатой под серверную.

2.1.2 Тип доступа для ЛВС

В рассматриваемой информационной системе решаются задачи, требующие интенсивного сетевого графика: связанные с обработкой, отображения и хранения документов, интеллектуального характера, принятия решений. Поэтому требуемая скорость работы в сети не менее 100Мб/с.

2.1.3 Выбор среды передачи и топологии сети

Так как требуемая скорость работы в сети не менее 100Мб/с, а топология «звезда-шина» 100Base-FX Ethernet – стандарт, использующий многомодовое волокно. Максимальная длина сегмента 400 метров в полудуплексе (для гарантированного обнаружения коллизий) или 2 километра в полном дуплексе. Название одномодовое или многомодовое волокно произошло от количества мод или, другими словами, траекторий распространения светового импульса при прохождении его по оптоволокну. В одномодовом оптоволокне образуется небольшое количество мод и условно считается, что свет в одномодовом

оптоволокне распространяется по одной траектории, поэтому такие оптические волокна называют одномодовыми. В многомодовом оптоволокне образуется большое число мод, поэтому такие волокна называют многомодовыми. У одномодового оптоволокна СКС диаметр сердцевины составляет 8-10 мкм. Для идентификации оптического кабеля с одномодовыми оптоволонами на кабеле можно встретить надписи 9/125 или 8-10/125.

Также будет использоваться беспроводное подключение по стандарту 802.11, так как в организации предусмотрено открытое рабочее пространство, где могут работать приглашенные сотрудники других подведомственных организаций «ГАУ ДПО «АмИРО»» на ноутбуках.

2.1.4 Выбор сетевой операционной системы

Правильный выбор сетевой ОС позволит уменьшить затраты на управление и администрирование, облегчит развитие организации и внедрение новых технологий, существенно повысит отдачу от вложений в аппаратные средства, а также предотвратит возможные проблемы благодаря сочетанию высокой надежности и эффективной защиты.

Сетевая операционная система масштаба предприятия прежде всего должна обладать основными свойствами любых корпоративных продуктов, в том числе:

а) масштабируемостью, то есть способностью одинаково хорошо работать в широком диапазоне различных количественных характеристик сети;

б) совместимостью с другими продуктами, то есть способностью работать в сложной гетерогенной среде интерсети в режиме plug-and-play.

Под данные критерии подходит ОС Ubuntu Server 20.04 LTS.

LTS расшифровывается как Long-Term Support или длительный срок поддержки. Это значит, что приложение или операционная система будет получать обновления безопасности и иногда даже обновления функциональности в течение более длительного периода времени, чем обычно.

LTS версии дистрибутивов и программ считаются очень стабильными, ведь они проходят тщательное тестирование перед выпуском. Важно отметить, что LTS версия не обязательно будет получать обновления функциональности, но гарантировано получит обновления безопасности и исправления ошибок. Такие системы рекомендуется использовать для производства, бизнеса и предприятий, потому что они будут поддерживаться на протяжении нескольких лет и в них не будут вноситься критические изменения.

2.1.5 Выбор сетевых протоколов

Выбор сетевых протоколов напрямую связан с сетевой ОС. Стек TCP/IP изначально создавался для глобальной сети, он имеет много особенностей, дающих ему преимущество перед другими протоколами, когда речь заходит о глобальных связях. Это способности фрагментации пакетов, гибкая система адресации, простота широковещательных запросов.

Сегодня набор протоколов TCP/IP самый распространённый протокол вычислительных сетей, поэтому мы его и выбираем.

2.1.6 Выбор платы сетевого адаптера

Следующий шаг – выбор платы сетевого адаптера, который зависит от вида сетевых протоколов, методов доступа к вычислительным сетям и используемой сетевой ОС. Выбор платы сетевого адаптера оказывает непосредственной влияние на производительность ЛВС. Если установлена медленная плата, то и скорость передачи информации по сети будет далека от высоких показателей. Кроме того, в сети с топологией шина, где нельзя начать передачу, пока кабель занят, медленная сетевая плата увеличивает время ожидания для всех пользователей. Выбирая плату сетевого адаптера, необходимо обратить внимание на те факторы, которые могут оказать влияние на функциональные возможности платы. К факторам, влияющих на скорость передачи данных относятся:

а) прямой доступ к памяти. Данные напрямую передаются из буфера платы сетевого адаптера в память компьютера, не затрагивая при этом центральный процессор;

б) разделяемая системная память. Процессор платы сетевого адаптера использует для обработки данных часть памяти компьютера;

в) управление шиной. К плате сетевого адаптера временно переходит управление шиной компьютера. Без использования ЦПУ плата передает данные непосредственно в системную память компьютера. При этом повышается производительность компьютера, поскольку его процессор в это время может решать другие задачи;

г) буферизация. Для большинства плат сетевого адаптера современные скорости передачи данных по сети слишком высоки. Поэтому на плате сетевого адаптера устанавливается буфер с помощью микросхем памяти. В случае, когда плата принимает данных больше, чем способна обработать, буфер сохраняет данные до тех пор, пока они не будут обработаны адаптером;

д) встроенный микропроцессор. С таким микропроцессором плате сетевого адаптера для обработки данных не требуется помощь компьютера;

е) серверы. С серверами связана значительная часть сетевого трафика, поэтому они должны быть оборудованы платами сетевого адаптера с наибольшей производительностью;

ё) рабочие станции. Рабочие станции могут использовать менее дорогие сетевые платы, если их работа с сетью ограничена приложениями, генерирующими небольшой объем сетевого трафика (например, текстовыми процессорами). Другие приложения (например, базы данных или инженерные приложения) довольно быстро перегрузят сетевые платы, не отвечающие их требованиям.

В нашем случае сетевые контроллеры встроены в платформу сервера. (Intel X722 + PHY Intel X557)

2.1.7 Сетевая печать

Так или иначе, но все пользователи сети печатают документы. Поэтому существует необходимость ввода в структуру ЛВС сетевых принтеров. Для определения расположения таких принтеров выявляются пользователи из тех, кто печатает больше остальных, рядом с ними и размещают сетевые принтеры,

либо учитывается наибольшая концентрация пользователей и сетевые принтеры ставятся в места наибольшего сосредоточения сотрудников.

2.1.8 Анализ полученных вариантов конфигурации ЛВС

Проанализировав вышеизложенную информацию, рассмотрим несколько вариантов, а затем выберем лучший. Результаты анализа всех возможных параметров сети и формирование различных конфигураций сети отображены в таблице 1.

Таблица 1 – Варианты конфигурации сети

Наименование параметра	Первый вариант	Второй вариант
Количество компьютеров	13	13
Тип сети	на основе выделенного сервера	на основе выделенного сервера
Количество серверов	2	2
Тип доступа к сети Топология сети	100Base-SX Ethernet звезда-шина	100Base-FX Ethernet звезда-шина
Среда передачи	Оптоволокно	Оптоволокно
Операционная система	Ubuntu Server 20.04 LTS	Ubuntu Server 20.04 LTS
Сетевые протоколы	TCP/IP	TCP/IP
Сетевые приложения	1. SoftEther VPN	1. SoftEther VPN
Сетевая печать	4 сетевых принтера, подключенных к серверу печати	4 принтера, подключенных к рабочим станциям
Подключение к глобальной сети	Выход в Интернет: ADSL- подключение по оптоволокну	Подключения ЛВС к спутниковому провайдеру с использованием аппаратных DVB-маршрутизаторов
Наличие средств безопасности	Фаервол - Outpost Firewall Pro 4.0, антивирусное ПО – Kaspersky Endpoint Security для бизнеса расширенный	Фаервол –Kerio, наличие серверной комнаты

Для выбора конфигурации сети необходимо решить задачу принятия решения в условиях полной определенности. Для этого далее рассмотрим стоимость сети, функциональные характеристики и средства защиты информации.

2.2 Проектирование структурной схемы вычислительной сети

Организация располагается на одном этаже в двухэтажном здании. Есть возможность организовать серверную. На этаже 3 кабинета.

Проведя анализ, была выбрана совокупность технических средств. В таблице 2 представлены технические средства, необходимые для функционирования сети.

Таблица 2 – Технические средства вычислительной сети

Наименование ТС	Цена, руб.	Количество, шт.	Стоимость, руб.
1	2	3	4
Платформа SuperMicro 4U 6049P-E1CR24L (LGA3647, C622, 3xPCI-E, SVGA, SAS/SATA RAID,24xHS SAS/SATA, 2x10GbLAN, 16DDR4 1200W HS)	175981.67	1	175981.67
Процессор CPU Intel Xeon Gold 5220 2.2 GHz LGA3647	116914.17	1	116914.17
Жёсткий диск HDD 10 Tb SATA 6Gb/s Seagate IronWolf NAS <ST10000VN0004> 3.5" 7200rpm 256Mb	23090.00	8	184720.00
Накопитель SSD 240 Gb SATA 6Gb/s Micron 5200 MAX <MTFDDAK240TDN> 2.5" 3D TLC	10201.67	1	10201.67
Охладитель <SNK-P0068APS4> 2U (4пин, 3647, 54дБ, 8400 об/мин,Cu+Al+тепловые трубки)	2804.17	1	2804.17
Модуль памяти Kingston <KSM24RS4/16MEI> DDR4 RDIMM 16Gb <PC4-19200> CL17 ECC Registered	6780.83	4	27123.32
Услуги по доставке и сборке сервера	100000	1	100000
Автоматизированное рабочее место (компьютер в сборе с гарнитурой)	80 000,00	3	240 000
Автоматизированное рабочее место (компьютер в сборе с гарнитурой)	70 000,00	10	700 000

Продолжение таблицы 2

1	2	3	4
Многофункциональное устройство	25 000,00	6	150 000
Маршрутизатор (WI-Fi роутер)	4 000,00	3	12 000
Коммутаторы Cisco SG110-16-E	10 999	3	32 997
Кабель оптоволокно 9A/125/900	3,3	1000 м	3300
Патч-кабель RJ-45 - RJ-45 категория 5+ (2 метра)	60	30	1800
Итого			1757842

В таблице 3 представлено необходимое сетевое программное обеспечение.

Таблица 3 – Сетевое программное обеспечение

Тип программного обеспечения	Наименование оборудования	Количество, шт.	Цена за единицу, руб.	Общая стоимость, руб.
Сетевая операционная система	Ubuntu Server 20.04 LTS	1	0	0
Сервер VPN	SoftEther VPN	1	0	0
Фаервол	Outpost Firewall Pro 4.0	1	10000	10000
Антивирусная программа	Kaspersky Endpoint Security для бизнеса расширенный	13	27860	362180
Офисные программы	Microsoft Office Home and Business 2010	13	18500	240500
Итого				612680

3 ПРОЕКТИРОВАНИЕ МОДУЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

3.1 Анализ предметной области

Анализ предметной области и актуальность вводимого модуля рассмотрены выше.

3.1.1 Анализ использования программно-технических средств

Предприятие оснащено современными средствами хранения, передачи и обработки информации. Локальная сеть, соединяющая все компьютеры и обеспечивающая доступ в сеть Интернет. Программные продукты, используемые предприятием представлены в таблице 4.

Таблица 4 – ПО, используемое на предприятии

Наименование программно-технического средства	Место установки	Основные функции
Kaspersky Endpoint Security для бизнеса - Стандартный Russian Edition.	Все подразделения	Комплексная защита на всех каналах поступления и передачи информации
ОС Windows 10	Все подразделения	Операционная система
Браузер Chrome	Все подразделения	Браузер для просмотра интернет-ресурсов
WinRar	Все подразделения	Архиватор файлов
Microsoft Office	Все подразделения	Офисный пакет приложений

3.1.2 Анализ существующей ИС

В данный момент в организации существует локальная вычислительная сеть (ЛВС) на основе клиент- серверной архитектуры. Так же ведется работа с ИС « Навигатор».

3.1.3 Обоснование необходимости создания модуля

Разработанный модуль отличается от аналогов, таких как распространенные мессенджеры WhatsApp, Telegram и прочие, простотой, бесплатностью использования и безопасностью, так как достоверно известно на каком сервере обрабатываются и хранятся сообщения. Для работы приложение требует минимальное количество ресурсов, при этом оно свободно от сторонних и мешающих не рабочих чатов. Экономически данное решение является также максимально выгодно, так как не требует покупки. Приложение можно активировать на множестве компьютеров предприятия, не боясь переплатить. Также данная программа очень дружелюбна и проста для пользователя, что позволяет работать в программе как опытным пользователям, так и новичкам в работе с персональным компьютером. Для работы пользователю нужно знать лишь основы компьютерной грамотности.

На основе этого можно сделать вывод, что приложение крайне выгодно для использования на предприятии в соотношении цена- качество.

В ходе исследования предприятия были изучены его организационная и функциональная структуры, а также внешний и внутренний документооборот предприятия. Помимо этого, было проанализировано программно- техническое оснащение « РМЦ». В результате исследования было принято решение разработать модуль локального чата, который облегчит работу и коммуникацию сотрудников предприятия.

3.2 Проектирование модуля ИС

3.2.1 Анализ требований к модулю ИС

3.2.1.1 Требования к структуре и функционированию

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

Авторизация пользователей;

Возможность отправить сообщение в общий чат организации

3.2.1.2 Требования к численности и квалификации персонала

Минимальное количество персонала, требуемого для работы программы, должно составлять не менее 2 штатных единиц - системный администратор и конечный пользователь программы - оператор.

Системный администратор должен иметь минимум среднее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

а) задача поддержания работоспособности технических средств;

б) задачи установки (инсталляции) и поддержания работоспособности системных программных средств - операционной системы;

в) задача установки (инсталляции) программы.

Конечный пользователь программы (оператор) должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы.

Персонал должен быть аттестован минимум на II квалификационную группу по электробезопасности (для работы с конторским оборудованием).

3.2.1.3 Требования к надежности

Надежное (устойчивое) функционирование программы должно быть обеспечено выполнением совокупности организационно- технических мероприятий:

а) организацией бесперебойного питания технических средств;

б) выполнением рекомендаций Министерства труда и социального развития РФ, изложенных в Постановлении от 23 июля 1998 г. « Об утверждении межотраслевых типовых норм времени на работы по сервисному обслуживанию ПЭВМ и оргтехники и сопровождению программных средств»;

в) выполнением требований ГОСТ 51188–98. Защита информации. Испытания программных средств на наличие компьютерных вирусов;

Обеспечиваются стороной- заказчиком.

3.2.1.4 Требования к интерфейсу пользователя

Система должна иметь человеко- машинный интерфейс, удовлетворяющий следующим требованиям:

– взаимодействие системы и пользователя должно осуществляться на русском языке, за исключением системных сообщений, не подлежащих русификации;

– должно быть реализовано отображение на экране только тех возможностей, которые доступны конкретному пользователю в соответствии с его функциональной ролью в системе;

– допустима видимость предоставляемой информации на экране;

– допустимая цветопередача.

3.2.1.5 Требования к эксплуатации, техническому обслуживанию, ремонту и хранению.

Пользователи обязаны быть проинформированы о правилах использования технических средств и работы с программой и с оборудованием, на котором используется данная программа.

Устройство хранения должно быть защищено от внешних физических воздействий, в качестве переноса и хранения может быть любой диск для хранения данных.

В случае аварии требования заключаются в сохранности информации при сбоях в работе системы, а также при допущении ошибок пользователей при работе с программой.

Программные средства администратора системы должны обеспечивать:

1 при выходе технических средств из строя, должна обеспечиваться ее замена без потери функциональной подсистемы;

2 полное или частичное восстановление потерянной информации;

3 протокол действий при возникновении нештатной ситуации.

3.2.1.6 Требования к информационному обеспечению и программной документации

Информационное обеспечение ИС должна содержать совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АС при ее функционировании. Информационный обмен между подсистемами должен обеспечиваться через использование общей базы данных.

Состав программной документации, предъявляемой на испытании:

- ГОСТ 19.402–78 – описание программы;
- ГОСТ 19.301-79 – программа и методика испытаний;
- ГОСТ 19.401-78 – тестирование программы.

3.2.1.7 Требования к лингвистическому обеспечению

Для создания данной программы необходимы знания языка программирования Python, знание о работе протоколов передачи данных.

3.2.1.8 Требования к программному обеспечению

Для реализации и эксплуатации модуля пользователь должен иметь установленную операционную систему семейства Windows не старше Windows XP.

3.2.1.9 Требования к техническому обеспечению

В состав технических средств должен входить IBM- совместимый персональный компьютер (ПЭВМ), включающий в себя:

1) процессор Pentium – 4 (AMD Athlon-64 X2) с тактовой частотой, 1.2 ГГц, не менее;
2) оперативную память объемом, 2 ГБ, не менее;
3) жесткий диск объемом 20 Гб, и выше;
4) манипулятор типа « мышь»;
5) наличие 1 COM- порта;
6) клавиатуру.

А также необходимы одна серверная платформа в качестве хранителя истории сообщений и обрабатывающий станции.

В случае работы системы в сети все компьютеры должны быть подобны. Так же необходимы кабеля для создания сети, сетевые карты на каждом компьютере и маршрутизатор.

3.2.3 Характеристика модуля « Локальный чат для сотрудников»

Чат предназначен для использования в локальной сети только указанной организации для быстрой связи между сотрудниками.

3.2.4 Описание вариантов использования

Диаграмма вариантов использования (сценариев поведения, прецедентов) является исходным концептуальным представлением системы в процессе ее проектирования и разработки. Данная диаграмма состоит из актеров, вариантов использования и отношений между ними.

Суть данной диаграммы состоит в том, что проектируемая система представляется в виде множества актеров, взаимодействующих с системой с помощью так вариантов использования. При этом актером (действующим лицом, актантом, актором) называется любой объект, субъект или система, взаимодействующая с моделируемой системой извне. В свою очередь вариант использования – это спецификация сервисов (функций), которые система предоставляет актеру. При этом в модели никак не отражается то, каким образом будет реализован этот набор действий.

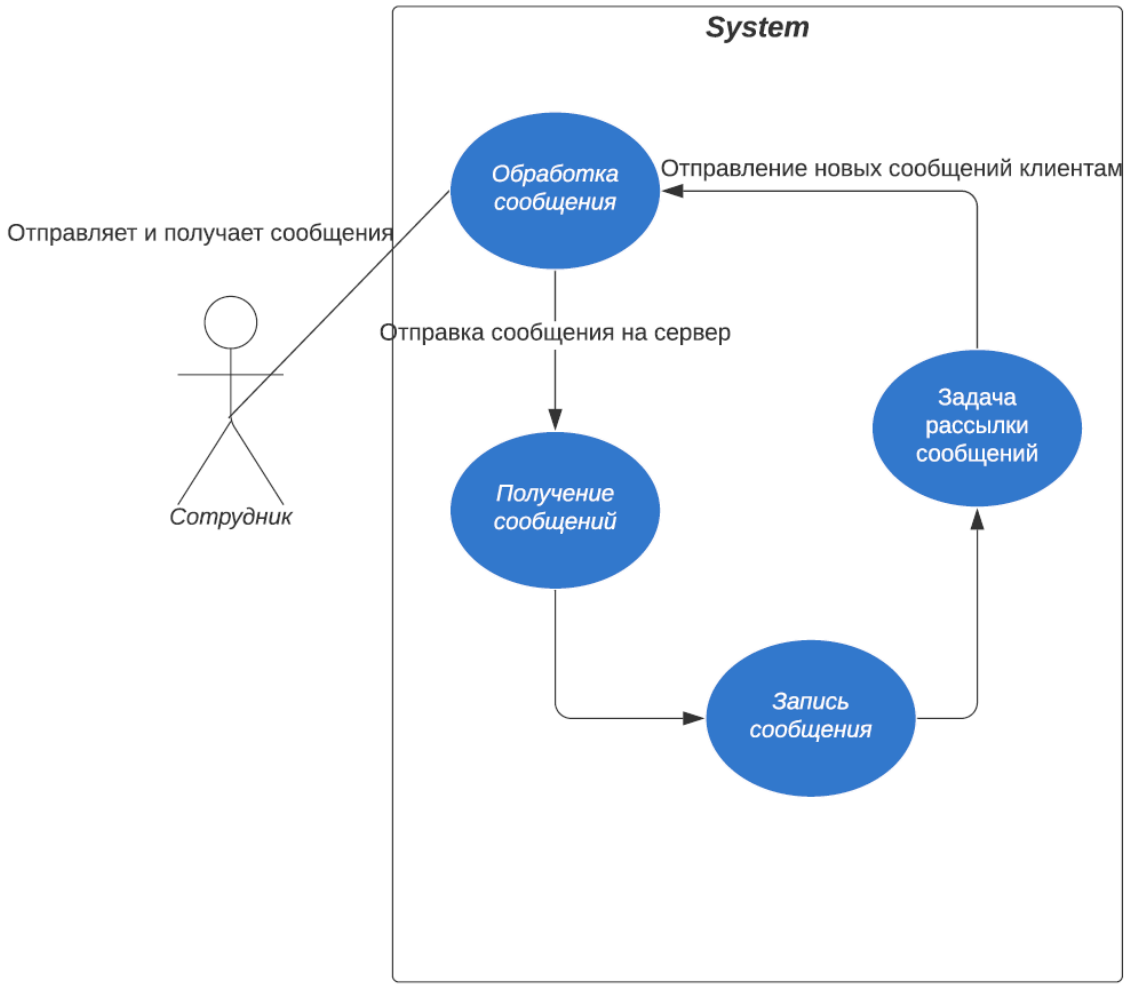

Рисунок 4 – диаграмма вариантов использования

Сотрудник вводит и отправляет сообщение на клиенте. Клиент в свою очередь отправляет сообщение, введенное пользователем на сервер, где сообщение записывается в специальный файл и затем задача рассылки отправляет новое сообщение всем клиентам в сети.

3.2.10 Задачи автоматизации, решаемые разрабатываемым модулем

При разработке данного модуля решалась задача быстрой и автоматизированной комуникации между сотрудниками в организации. После внедрения этого модуля больше нет необходимости всем сотрудникам находится в одном помещении и отвлекаться от выполнения своих задач, т.к. вся необходимая информация и поручения появляются прямо на рабочем компьютере.

4 РАЗРАБОТКА МОДУЛЯ

4.1 Описание программного модуля

Данный модуль создается для автоматизации процесса коммуникации между сотрудниками и распространение распоряжений от директора организации. Программный продукт позволяет обмениваться мгновенными сообщениями.

4.2 Обоснование выбора языка программирования

В качестве основного языка программирования был выбран язык программирования Python. Сейчас это один из самых популярных языков по статистике сайта tiobe. com и используется он практически во всех сферах деятельности (рис. 5).

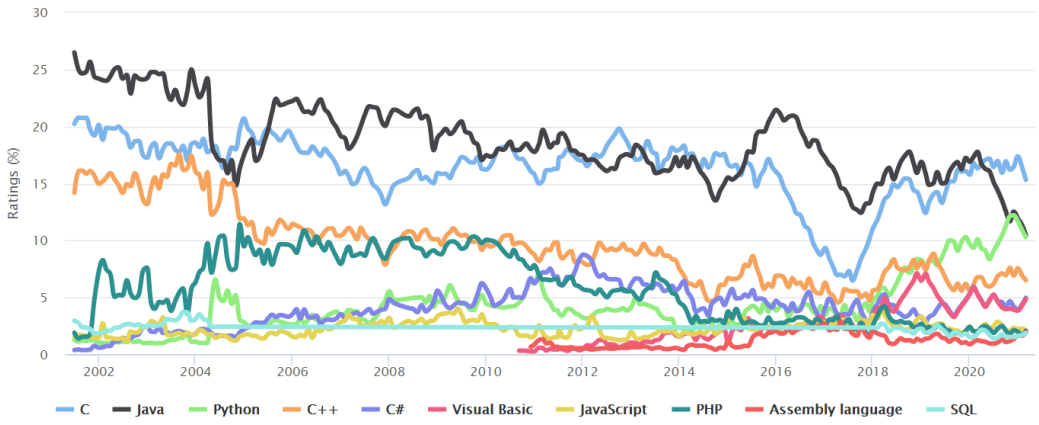

Рисунок 5 – статистика популярности языков программирования

Python имеет множество библиотек для работы с клиент – серверной архитектурой, протоколов передачи данных, обработки запросов и многого другого. В работе используется такие библиотеки как:

– библиотека Requests для упрощения работы с веб- приложениями и HTTP- протоколами;

– библиотека Flask — фреймворк для создания веб- приложений, использующий набор инструментов Werkzeug, а также шаблонизатор

Jinja2. Относится к категории так называемых микрофреймворков — минималистичных каркасов веб- приложений, сознательно предоставляющих лишь самые базовые возможности;

– библиотека json для кодирования и декодирования объектов в удобном для чтения формате;

– библиотеки datetime и time для работы с форматами времени.

Так же необходимо, чтобы пользователям было удобно и интуитивно понятно, как пользоваться предложенным приложением. Для этого было использовано приложение Qt Designer. Это приложение предоставляет возможность создания и редактирования форм, которые в последствии связываются непосредственно с написанным кодом при помощи специальной библиотеки PyQt6. У этой библиотеки есть методы, которые позволяют отлавливать события, такие как:

– движение курсора мыши;

– нажатия кнопок, размещенных на созданной форме;

– нажатия на определенные клавиши клавиатуры и так далее

4.3 Алгоритм функционирования программы

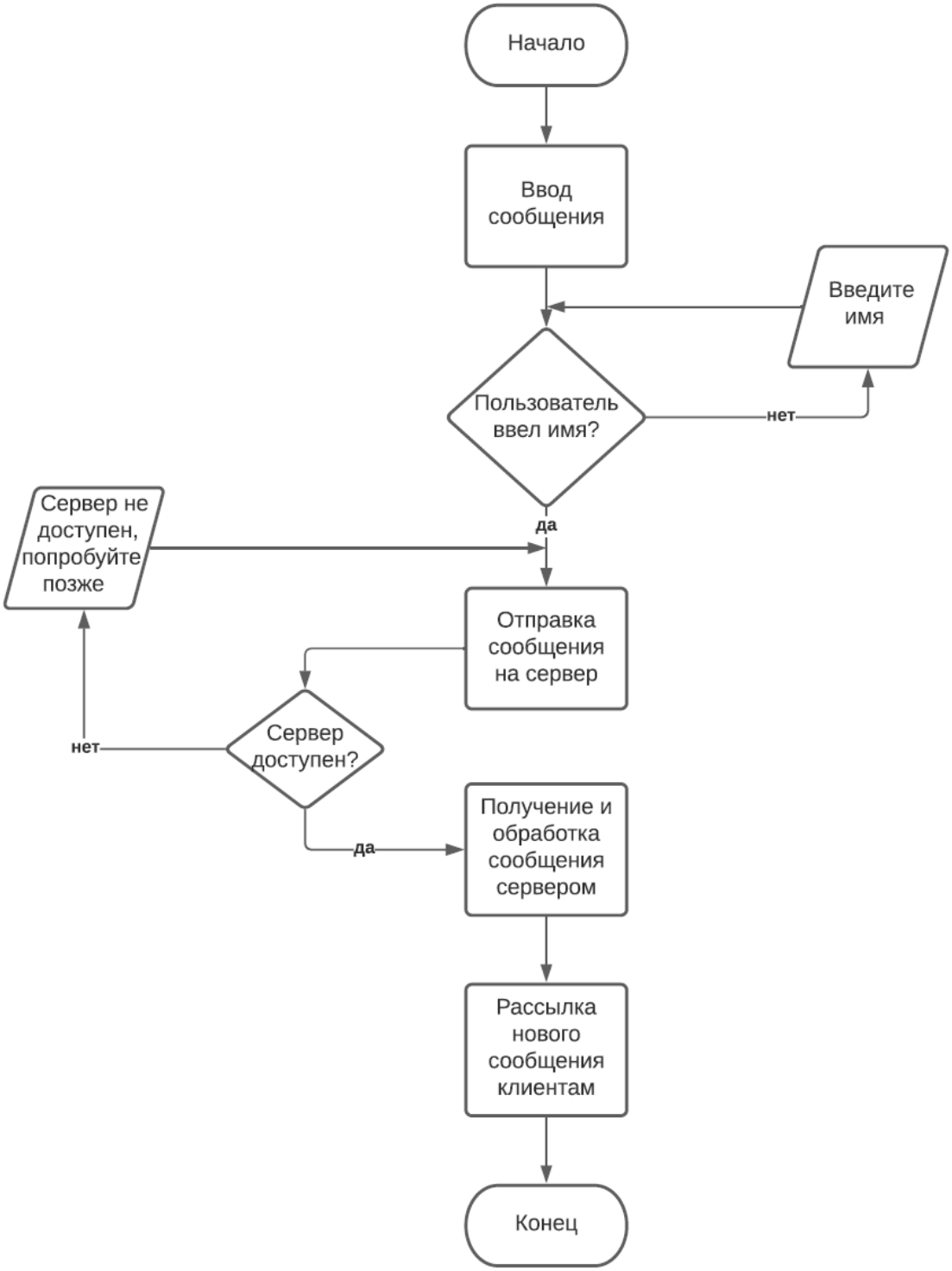

Рисунок 6 – упрощенная схема функционирования модуля

На рисунке 6 представлена упрощенная схема функционирования модуля. Упрощенной она является потому, что не все алгоритмы проверки и обработки исключений показаны на ней.

Алгоритм начинается с интерфейса клиента, где пользователь проходит идентификацию, вводит и отправляет сообщение. После нажатия кнопки отправки сообщения клиент проверяет доступность сервера и, если он доступен, отправляет ему сообщение. Сервер получает его и проверяет правильность и корректность полученного сообщения, затем записывает его в файл и рассылает его всем клиентам.

4.4 Функции модуля

При запуске клиентской части приложения пользователя встречает окно мессенджера.

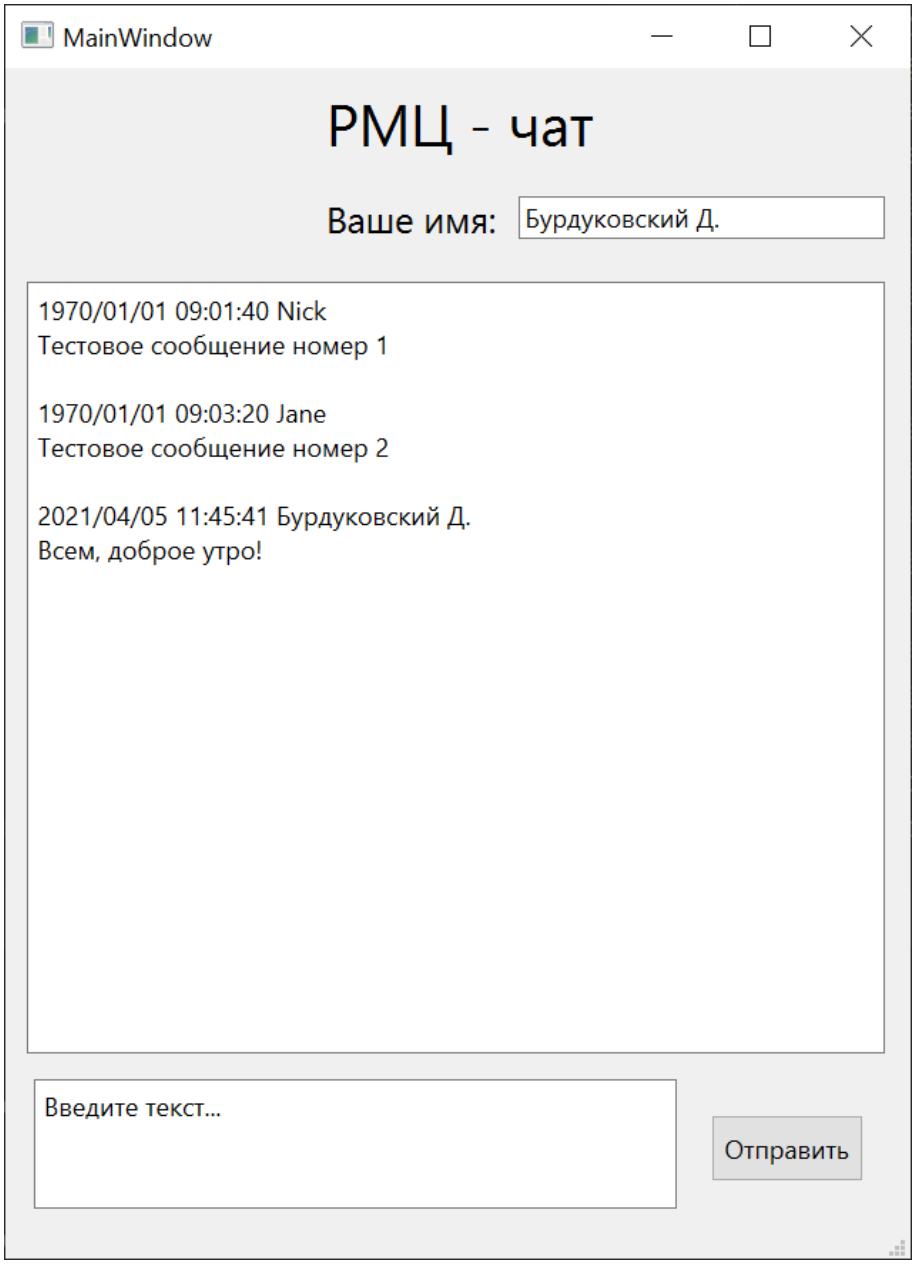

Рисунок 7 – Окно мессенджера

Серверная часть представляет собой файл языка Python. Так как в организации локальный сервер работает на linux- подобной операционной системе, а такие системы уже включают в себя интерпретатор языка Python и, соответственно, серверную часть можно запустить непосредственно из строки терминала. Так же подразумевается, что системный администратор владеет основами программирования и сможет при необходимости изменить конфигурацию серверной части приложения.

```
(venv) D:\Python\pythonProject\pythonProject\mess>py server.py
 * Serving Flask app "server" (lazy loading)
 * Environment: production
   WARNING: This is a development server. Do not use it in a production deployment.
   Use a production WSGI server instead.
 * Debug mode: off
 * Running on http://127.0.0.1:5000/ (Press CTRL+C to quit)
127.0.0.1 - - [05/Apr/2021 11:44:51] "←[37mGET /messages?after=0 HTTP/1.1←[0m" 200 -
127.0.0.1 - - [05/Apr/2021 11:44:52] "←[37mGET /messages?after=200 HTTP/1.1←[0m" 200 -
127.0.0.1 - - [05/Apr/2021 11:44:53] "←[37mGET /messages?after=200 HTTP/1.1←[0m" 200 -
127.0.0.1 - - [05/Apr/2021 11:44:54] "←[37mGET /messages?after=200 HTTP/1.1←[0m" 200 -
```

Рисунок 8 – запуск и работа серверной части

5 БЕЗОПАСНОСТЬ

5.1 Информационная безопасность

Защита информации включает в себя комплекс мероприятий, направленных на обеспечение информационной безопасности в организации.

Всем защитным мерам должен предшествовать анализ угроз и составления модели угроз. Модель угроз представлена в Приложении Б. К числу угроз можно отнести все, что влечет за собой потерю данных в сети, а также:

а) воровство или вандализм;

б) пожар;

в) отказы источников питания и скачки напряжения;

г) отказы компонентов;

д) природные явления (молния, наводнения, бури и землетрясения).

На сегодняшний день сформулировано три основных принципа информационной безопасности:

а) целостность данных;

б) конфиденциальность информации;

в) доступность информации для всех авторизованных пользователей.

Для защиты информации будем использовать следующие средства:

а) физические средства защиты информации. К ним относятся ограничение или полный запрет доступа посторонних лиц на территорию, пропускные пункты, оснащенные специальными системами;

б) базовые средства защиты электронной информации. Это незаменимый компонент обеспечения информационной безопасности. К ним относятся антивирусные программы, а также системы фильтрации электронной почты, защищающие пользователя от нежелательной или подозрительной корреспонденции;

в) резервное копирование данных. Это решение, подразумевающее хранение важной информации не только на конкретном компьютере, но и на сервере;

г) шифрование данных при передаче информации в электронном формате. Чтобы обеспечить конфиденциальность информации при ее передаче в электронном формате применяются различные виды шифрования. Шифрование дает возможность подтвердить подлинность передаваемой информации, защитить ее при хранении на открытых носителях, защитить ПО и другие информационные ресурсы компании от несанкционированного копирования и использования

Лишь при комплексном подходе к защите информации, реализации как можно большего количества выше представленных средств можно свести к минимуму вероятность возникновения угроз и утечек.

Необходимой функцией средств обеспечения безопасности является регистрация деятельности пользователей. Для каждой базы данных, отдельного документа и даже отдельного поля записи в файле базы данных могут быть установлены:

а) список пользователей, имеющих право доступа;

б) функции, которые может выполнять пользователь;

в) привилегии для доступа к выбранной информации.

В проектируемой ЛВС выборочно наделим пользователей соответствующими правами доступа к каталогам и создадим группы для предоставления доступа к общим сетевым ресурсам (таблица 4).

Таблица 5 – Права пользователей ЛВС

Название группы	Внутренние ресурсы	Уровни доступа к внутренним ресурсам	Доступ в Internet
1	2	3	4
Администратор	Все сетевые ресурсы	Все права администратора в каталогах, в том числе изменение уровня, прав доступа	Все сетевые ресурсы
Директор и его заместители	Файловая система	Создание, чтение файлов, запись в файл, создание подкаталогов и файлов, удаление каталогов	Все сетевые ресурсы

Продолжение таблицы 5

1	2	3	4
Методический кабинет	Файловая система	Ограничение доступа к папкам (по функциональным обязанностям)	Ограничение по IP-адресу (адресата и источника), ограничение по содержанию (входящий и исходящий
Администраторы « Навигатора»	Файловая система	Ограничение доступа к папкам (по функциональным обязанностям)	Ограничение по IP-адресу (адресата и источника), ограничение по содержанию (входящий и исходящий трафик), аутентификация удаленного пользователя.
Экономист	Файловая система	Ограничение доступа к папкам (по функциональным обязанностям)	Ограничение по IP-адресу (адресата и источника), ограничение по содержанию (входящий и исходящий трафик), аутентификация удаленного пользователя.
Специалист по рекламе и педагог организатор	Файловая система	Ограничение доступа к папкам (только общие файлы)	Ограничение по IP-адресу (адресата и источника), ограничение по содержанию (входящий и исходящий трафик), аутентификация удаленного пользователя.
Гость	Файловая система	Ограничение доступа к папкам только общедоступные файлы)	Ограничение по IP-адресу (адресата и источника), ограничение по содержанию (входящий и исходящий трафик), аутентификация удаленного пользователя.

5.2 Безопасность и экологичность

Система сохранения жизни и здоровья работников в процессе трудовой деятельности называется охрана труда. Данная система включает в себя правовые, санитарно- гигиенические, лечебно- профилактические, социально- экономические, организационно- технические, реабилитационные и иные мероприятия. В данном разделе будут исследовано безопасность

жизнедеятельности сотрудников организации « ГАУ ДПО « АмИРО « Региональный модельный центр» Раздел будет состоять из 4 основных глав: безопасность, экологичность, чрезвычайные ситуации и комплексы физических упражнений.

5.2.1 Безопасность

5.2.1.1 Требования к ПЭВМ

В « РМЦ» в офисе конструкция ПЭВМ обеспечивает возможность поворота корпуса в вертикальной и горизонтальной плоскости с фиксацией в определенном положении для обеспечения фронтального наблюдения экрана ВДТ. Корпус ПЭВМ, клавиатура и другие устройства ПЭВМ имеют матовую поверхность и не имеют блестящих деталей, способных создавать различные блики. Конструкция ВДТ предусматривает регулирование яркости и контрастности. ПЭВМ соответствуют рекомендациям, описанных в пособии о безопасной работе на персональных компьютерах.

Так же любой ПЭВМ должен иметь сертификат – это документ, устанавливающий соответствие компьютерной техники нормам безопасности, качества, утверждённым законом. Установленные в компании ПЭВМ имеют сертификаты.

5.2.1.2 Требования к помещению

Все помещения оснащены регулируемыми жалюзи. Площадь помещений от большего к малому составляет 60м^2, 54,4м^2, 44,1м^2, 28,3м^2 и 16,6м^2. Помещения оборудованы защитным заземлением. Минимальная площадь одного рабочего места должно соответствовать 4,5м^2 при использовании монитора с плоским экраном, и 6м^2 при использовании монитора с лучевой трубкой. Площадь одного рабочего места составляет 5 м2. Влажная уборка и проветривание проводится в помещениях следуя установленному графику.

После анализа помещения было выявлено что все рабочие места размещены согласно требованиям учебного пособия « Эргономика рабочих

мест служащих и инженерно- технических работников, оснащенных ПЭВМ».

5.2.1.3 Требования к рабочему месту

Рабочее место каждого сотрудника состоит из рабочего кресла, рабочего стола, тумбы и персонального компьютера. Высота рабочего стола сотрудника составляет 0,73 м, ширина – 1,4 м, а также его глубина – 0,9 м. Рабочий стол имеет пространство для ног с высотой 0,65 м, шириной – 0,6 м и глубиной на уровне колен – 0,55 м и на уровне вытянутых ног – 0,71 м. Конструкция рабочего стула обеспечивает:

- поверхность сиденья с закругленным передним краем;
- возможность регулировать высоту поверхности сидения от 0,4 м до 0,5 м и углы наклона вперёд до 13 градусов, и назад до 4 градусов.;
- ширина и глубина поверхности сиденья составляет 0,55 м;
- высота опорной поверхности спинки составляет 0,32 м, ширина – 0,45 м, угол наклона в вертикальной плоскости – 25 градусов.

Экран видеомонитора находится от глаз пользователя на расстоянии 0,7 м. Клавиатура располагается на расстоянии 0,15 от края, обращенного к пользователю на поверхности рабочего стола.

Температура воздуха на рабочем месте в холодный период года от 20 °С до 23 °С, в теплый период от 21 °С до 25 °С. Относительная влажность составляет от 45 % до 60 %, скорость движения воздуха – 0,1 м/с. Для выполнения установленных норм в помещениях установлены система кондиционирования воздуха и система отопления.

5.2.1.4 Режим труда и отдыха при работе с компьютером

Основные виды трудовой деятельности на персональном компьютере подразделяются на 3 группы: группа А – работа по считыванию информации с экрана; группа Б – работа по вводу информации; группа В – творческая работа в режиме диалога с персональным компьютером.

В течении рабочей смены пользователь выполняет различные виды работ, следовательно, его относят к той группе работ на которую он тратит 50% и более времени рабочей смены.

Все сотрудники относятся ко всем 3 группам, так как выполнение работ можно представить в процентном соотношении, 33% на каждый вид работ в течении всей рабочей смены.

Также существуют категории тяжести и напряженности работы на персональном компьютере. Данные виды категорий представлены в таблице 6.

С помощью таблицы 6 можно сказать, что сотрудники компании относятся ко второй категории тяжести и напряженности работы.

Таблица 6 - Категории тяжести и напряженности работы

Группа	Категории тяжести и напряженности работы		
	I	II	III
А (по числу считываемых знаков за смену)	До 20 тыс.	До 40 тыс.	До 60 тыс.
Б (по числу считываемых или вводимых знаков за смену)	До 15 тыс.	До 30 тыс.	До 40 тыс.
В (по суммарному времени непосредственной работы с ПЭВМ)	До 2 ч	До 4 ч	До 6 ч

В « РМЦ» 8- ми часовая рабочая смена поэтому перерывы следует устанавливать:

- 1 категория работ – через 2 часа от начала смены и через 2 часа после обеденного перерыва продолжительностью 15 минут каждый;

- 2 категория работ – через 2 часа от начала рабочей смены и через 1,5- 2,0 часа после обеденного перерыва продолжительностью 15 минут каждый или продолжительностью 10 минут через каждый час работы;

- 3 категория работ – через 1,5-2,0 часа от начала рабочей смены и через 1,5-2,0 часа после обеденного перерыва продолжительностью 20 минут каждый или продолжительностью 15 минут через каждый час работы.

Труд всех сотрудников организации относится к третьей категории тяжести работы.

5.2.2 Экологичность

Экологичность – качество чего- либо, отражающее его способность не наносить вреда окружающей природе. Конструкция ПЭВМ состоит из многих компонентов. Данные компоненты содержат токсичные вещества, которые вредны для окружающей среды и для человека.

Для обеспечения экологичности в организации ГАУ ДПО « АмИРО» « Региональный модельный центр» существует Федеральный закон №89 « Об отходах производства и потребления» от 24.06.1998 (ред. От 28.12.2016). Данным законом регулируются способы утилизации отходов.

Для утилизации макулатуры, необходимо в специальном помещении измельчить бумагу с помощью технических устройств. Затем оставить на хранении до передачи в пункт приема макулатуры. В Благовещенске этим занимается – ОАО « Вторресурсы». Самостоятельная утилизация данных отходов, то есть сжигание, закапывание не допускается.

Для утилизации компьютерной техники в Благовещенске необходимо обратиться в компанию – ООО « ФПК- СЕРВИС».

Лампы дневного света содержат ртуть. А это вещество относится к первому классу опасности. Пары ртути поражают печень, почки, центральную нервную систему. Ртутную лампу нельзя утилизировать вместе с бытовыми отходами. В Благовещенске по вопросам утилизации ртутьсодержащих отходов можно обратиться в ООО « Центр демеркуризации».

Каждый компьютер, а также оргтехника содержит на только ценные цветные металлы, но и целый набор опасных для окружающей среды веществ. Это производные газов, тяжелые металлы, среди которых кадмий,

ртуть и свинец. Попадая на свалку, все эти вещества под воздействием внешней среды постепенно проникают в почву, отравляют воздух и воду.

Утилизируемое оборудование хранится в подсобном помещении, так как при хранении оно не выделяет вредных веществ, поэтому может храниться в открытом виде. Транспортируется к месту утилизации, так же в открытом виде, на заднем сидении машины сотрудника.

Утилизацией данного оборудования в городе Благовещенске занимается ООО « ФПК- СЕРВИС».

Так же в процессе трудовой деятельности компании, активно используются источники бесперебойного питания, в которых используются свинцовые аккумуляторные батареи, которые так же после выхода из строя, подлежат утилизации.

Вышедшие из строя аккумуляторы, хранятся в том же подсобном помещении, где и утилизируемая компьютерная техника. При накоплении трех аккумуляторов, они вывозятся компанией утилизатором.

Утилизацией аккумуляторных батарей в городе Благовещенске занимается ООО « Метэко».

5.2.3 Чрезвычайные ситуации

При работе в помещении за компьютером могут произойти различные чрезвычайные ситуации: пожар, взрыв в здании, разрушение здания от сейсмической активности, затопление, получение урона от электрического тока.

Наиболее вероятная чрезвычайная ситуация для помещения - пожар.

В помещении специалистов технического блока существует электропроводка напряжением 220 вольт, которая обеспечивает питанием все электроприборы, а также систему освещения. При коротком замыкании или неправильной эксплуатации устройств есть вероятность того, что произойдёт возгорание, которое может нанести физический вред как всему персоналу, так и оборудованию.

В соответствии с техническим регламентом о требованиях пожарной безопасности на предприятии проводятся следующие пожарно- профилактические мероприятия:

- организационные мероприятия, касающиеся технического процесса с учетом пожарной безопасности объекта;

- эксплуатационные мероприятия, рассматривающие эксплуатацию имеющегося оборудования;

- технические и конструктивные, связанные с правильным размещением и монтажом электрооборудования и отопительных приборов.

Рассмотрим каждые пожарно- профилактические мероприятия поподробнее.

Организационные мероприятия содержат:

- обучение персонала правилам техники безопасности;

- противопожарный инструктаж обслуживающего персонала;

- издание плакатов, инструкций, планов эвакуации. Эксплуатационные мероприятия включают в себя:

- соблюдение эксплуатационных норм оборудования;

- обеспечение свободного подхода к оборудованию;

- содержание в исправном состоянии изоляции токоведущих проводников.

К техническим мероприятиям относится соблюдение противопожарных требований при устройстве оборудования, электропроводок, систем отопления, вентиляции и освещения.

Простым и быстрым средством пожаротушения является вода, поступающая из обычного водопровода, но так как в помещении используются электроприборы необходимо использовать песок. Для осуществления эффективного тушения огня используют пожарные рукава и стволы, находящиеся в специальных шкафах, расположенных в коридоре. В пунктах первичных средств огнетушения должны располагаться ящик с песком, пожарные ведра и топор.

Если возгорание произошло в электроустановке, для его устранения должны использоваться огнетушители углекислотные типа ОУ–2, или порошковые типа ОП–5. Кроме устранения самого очага пожара нужно, своевременно, организовать эвакуацию людей.

Комплекс организационных и технических мероприятий пожарной профилактики, таких как устройство эвакуационных путей, систем обнаружения пожара в случае возникновения пожара может обеспечить безопасность людей, ограничить распространение огня, предотвратить пожар, а также создать условия для успешного тушения пожара. В « РМЦ» реализована система пожарной безопасности в соответствии с техническим регламентом о пожарной безопасности.

5.2.4 Комплексы физических упражнений для сохранения и укрепления индивидуального здоровья и обеспечения полноценной профессиональной деятельности

Регламентированные микропаузы и перерывы целесообразно использовать для выполнения комплексов упражнений и гимнастики для глаз, для снятия утомления с плечевого пояса и рук, для улучшенного мозгового кровообращения. Через 2-3 недели следует менять комплексы упражнений.

5.2.4.1 Комплексы упражнений для глаз

Упражнения выполняются сидя или стоя, отвернувшись от экрана, при ритмичном дыхании, с максимальной амплитудой движения глаз.

Вариант 1:

1) закрыть глаза, сильно напрягая глазные мышцы, на счет 1 - 4, затем раскрыть глаза, расслабив мышцы глаз, посмотреть вдаль на счет 1 - 6. Повторить 4 - 5 раз;

2) посмотреть на переносицу и задержать взор на счет 1 - 4. До усталости глаза не доводить. Затем открыть глаза, посмотреть вдаль на счет 1 - 6. Повторить 4 - 5 раз;

3) не поворачивая головы, посмотреть направо и зафиксировать взгляд

На счет 1 - 4, затем посмотреть вдаль прямо на счет 1 - 6. Аналогичным образом проводятся упражнения, но с фиксацией взгляда влево, вверх и вниз. Повторить 3 - 4 раза;

4) перенести взгляд быстро по диагонали: направо вверх - налево вниз, потом прямо вдаль на счет 1 - 6; затем налево вверх направо вниз и посмотреть вдаль на счет 1 - 6. Повторить 4 - 5 раз.

Вариант 2:

1) закрыть глаза, не напрягая глазные мышцы, на счет 1 - 4, широко рас- крыть глаза и посмотреть вдаль на счет 1 - 6. Повторить 4 - 5 раз;

2) посмотреть на кончик носа на счет 1 - 4, а потом перевести взгляд вдаль на счет 1 - 6. Повторить 4 - 5 раз;

3) не поворачивая головы (голова прямо), делать медленно круговые движения глазами вверх- вправо- вниз- влево и в обратную сторону: вверх- влево- вниз- вправо. Затем посмотреть вдаль на счет 1 - 6. Повторить 4 - 5 раз;

4) при неподвижной голове перевести взор с фиксацией его на счет 1 - 4 вверх, на счет 1 - 6 прямо; после чего аналогичным образом вниз- прямо, вправо- прямо, влево- прямо. Проделать движение по диагонали в одну и другую стороны с переводом глаз прямо на счет 1 - 6. Повторить 3 - 4 раза.

5.2.4.2 Комплексы упражнений физкультурных минуток

Физкультминутка способствует снятию локального утомления. По содержанию Физкультминутки различны и предназначаются для конкретного воздействия на ту или иную группу мышц или систему организма в зависимости от самочувствия и ощущения усталости.

Физкультминутка общего воздействия может применяться, когда физкультпаузу по каким- либо причинам выполнить нет возможности. Существует определённые физкультминутки.

1 комплекс общего воздействия:

1) исходное положение (и.п.) - основная стойка (о.с.) 1 - 2 - встать

на носки, руки вверх- наружу, потянуться вверх за руками. 3 - 4 - дугами в стороны руки вниз и расслабленно скрестить перед грудью, голову наклонить вперед. Повторить 6 - 8 раз. Темп быстрый;

2) и.п. - стойка ноги врозь, руки вперед, 1 - поворот туловища направо, мах левой рукой вправо, правой назад за спину. 2 и.п. 3 - 4 - то же в другую сторону. Упражнения выполняются размашисто, динамично. Повторить 6 - 8 раз. Темп быстрый;

3) и.п. 1 - согнуть правую ногу вперед и, обхватив голень руками, притянуть ногу к животу. 2 - приставить ногу, руки вверх- наружу. 3 - 4 - то же другой ногой. Повторить 6 - 8 раз. Темп средний.

2 комплекс общего воздействия:

1) и.п. - о.с. 1 - 2 - дугами внутрь два круга руками в лицевой плоскости.

3 - 4 - то же, но круги наружу. Повторить 4 - 6 раз. Темп средний;

2) и.п. - стойка ноги врозь, правую руку вперед, левую на пояс. 1 - 3 - круг правой рукой вниз в боковой плоскости с поворотом туловища направо. 4 - заканчивая круг, правую руку на пояс, левую вперед. То же в другую сторону. Повторить 4 - 6 раз. Темп средний;

3) и.п. - о.с. 1 - с шагом вправо руки в стороны. 2 - два пружинящих наклона вправо. Руки на пояс. 4 - и.п. 1 - 4 - то же влево. Повторить 4 - 6 раз в каждую сторону. Темп средний.

Для улучшения мозгового кровообращения делаются наклоны и повороты головы оказывают механическое воздействие на стенки шейных кровеносных сосудов, повышают их эластичность; раздражение вестибулярного аппарата вызывает расширение кровеносных сосудов головного мозга. Все это усиливает мозговое кровообращение, повышает его интенсивность и облегчает умственную деятельность.

1 комплекс для улучшения мозгового кровообращения:

1) исходное положение (и.п.) - основная стойка (о.с.) 1 - руки за голову; локти развести пошире, голову наклонить назад. 2 - локти вперед.

3 - 4 - руки расслабленно вниз, голову наклонить вперед. Повторить 4 - 6 раз. Темп медленный;

2) и.п. - стойка ноги врозь, кисти в кулаках. 1 - мах левой рукой назад, правой вверх - назад. 2 - встречными махами переменить положение рук. Махи заканчивать рывками руками назад. Повторить 6 - 8 раз. Темп средний;

3) и.п. - сидя на стуле. 1 - 2 отвести голову назад и плавно наклонить назад. 3 - 4 - голову наклонить вперед, плечи не поднимать. Повторить 4 - 6 раз. Темп медленный.

2 комплекс для улучшения мозгового кровообращения:

1) и.п. - стоя или сидя, руки на поясе. 1 - 2 - круг правой рукой назад с поворотом туловища и головы направо. 3 - 4 - то же левой рукой. Повторить 4- 6 раз. Темп медленный;

2) и.п. - стоя или сидя, руки в стороны, ладони вперед, пальцы разведены.1 - обхватив себя за плечи руками возможно крепче и дальше. 2 - и.п. То же налево. Повторить 4 - 6 раз. Темп быстрый;

3) и.п. - сидя на стуле, руки на пояс. 1 - повернуть голову направо. 2 - и.п.То же налево. Повторить 6 - 8 раз. Темп медленный.

Для снятия утомления с плечевого пояса и рук помогают динамические упражнения с чередованием напряжения и расслабления отдельных мышечных групп плечевого пояса и рук улучшают кровоснабжение, снижают напряжение.

1 комплекс для снятия утомления с плечевого пояса и рук:

1) исходное положение (и.п.) - основная стойка (о.с.) 1 - поднять плечи. 2 - опустить плечи. Повторить 6 - 8 раз, затем пауза 2 - 3 с, расслабить мышцыплечевого пояса. Темп медленный;

2) и.п. - руки согнуты перед грудью. 1 - 2 - два пружинящих рывка назадсогнутыми руками. 3 - 4 - то же прямыми руками. Повторить 4 - 6 раз. Темп средний;

3) и.п. - стойка ноги врозь. 1 - 4 - четыре последовательных круга

рукаминазад. 5 - 8 - то же вперед. Руки не напрягать, туловище не поворачивать. Повторить 4 - 6 раз. Закончить расслаблением. Темп средний.

2 комплекс для снятия утомления с плечевого пояса и рук:

1) и.п. - о.с. - кисти в кулаках. Встречные махи руками вперед и назад.Повторить 4 - 6 раз. Темп средний;

2) и.п. - о.с. 1 - 4 - дугами в стороны руки вверх, одновременно делая иминебольшие воронкообразные движения. 5 - 8 - дугами в стороны руки расслаб-ленно вниз и потрясти кистями. Повторить 4 - 6 раз. Темп средний;

3) и.п. - тыльной стороной кисти на пояс. 1 - 2 - свести вперед, голову наклонить вперед. 3 - 4 - локти назад, прогнуться. Повторить 6 - 8 раз, затемруки вниз и потрясти расслабленно. Темп медленный.

Физические упражнения для мышц ног, живота и спины усиливают венозное кровообращение в этих частях тела и способствуют предотвращению застойных явлений крово- и лимфообращения, отечности в нижних конечностях.

1 комплекс для снятия утомления с туловища и ног:

1) исходное положение (и.п.) - основная стойка (о.с.) 1 - шаг влево, руки к плечам, прогнуться. 2 - и.п. 3 - 4 - то же в другую сторону. Повторить 6 - 8 раз. Темп медленный;

2) и.п. - стойка ноги врозь. 1 - упор присев. 2 - и.п. 3 - наклон вперед, руки впереди. 4 - и.п. Повторить 6 - 8 раз. Темп средний;

3) и.п. - стойка ноги врозь, руки за голову. 1 - 3 - круговые движения тазом в одну сторону. 4 - 6 - то же в другую сторону. 7 - 8 - руки вниз и расслабленно потрясти кистями. Повторить 4 - 6 раз. Темп средний.

2 комплекс для снятия утомления с туловища и ног:

1) и.п. - о.с. 1 - выпад влево, руки дугами внутрь, вверх в стороны. 2 - толчком левой приставить ногу, дугами внутрь руки вниз. 3 - 4 - то же в другую сторону. Повторить 6 - 8 раз. Темп средний;

2) и.п. - о.с. 1- 2 - присед на носках, колени врозь, руки вперед - в

стороны. 3 - встать на правую, мах левой назад, руки вверх, 4 - приставить левую, руки свободно вниз и встряхнуть руками. 5 - 8 - то же с махом правой ногой назад. Повторить 4 - 6 раз. Темп средний;

3) и.п. - стойка ноги врозь. 1 - 2 - наклон вперед, правая рука скользит вдоль ноги вниз, левая, сгибаясь, вдоль тела вверх. 3 - 4 - и.п. 5 - 8 - то же в другую сторону. Повторить 6 - 8 раз. Темп средний.

5.4.3 Комплексы упражнений физкультурных пауз

Физкультурная пауза - повышает двигательную активность, стимулирует деятельность нервной, сердечно- сосудистой, дыхательной и мышечной систем, снимает общее утомление, повышает умственную работоспособность.

Физкультурная пауза состоит из ряда различных упражнений:

1) ходьба на месте 20 - 30 с. Темп средний;

2) исходное положение (и.п.) - основная стойка (о.с.). 1 - руки вперед, ладони книзу. 2 - руки в стороны, ладони кверху, 3 - встать на носки, руки вверх, прогнуться. 4 - и.п. Повторить 4 - 6 раз. Темп медленный;

3) и.п. - ноги врозь, немного шире плеч. 1 - 3 наклон назад, руки за спину.

3 - 4 - и.п. Повторить 6 - 8 раз. Темп средний;

4) и.п. - ноги на ширине плеч. 1 - руки за голову, поворот туловища направо. 2 - туловище в и.п., руки в стороны, наклон вперед, голову назад. 3 - выпрямиться, руки за голову, поворот туловища налево. 4 - и.п. 5 - 8 - то же в другую сторону. Повторить 6 раз. Темп средний;

5) и.п. - руки к плечам. 1 - выпад вправо, руки в стороны. 2 - и.п. 3 - присесть, руки вверх. 4 - и.п. 5 - 8 - то же в другую сторону. Повторить 6 раз. Темп средний;

6) и.п. - ноги врозь, руки на пояс. 1 - 4 - круговые движения туловищем вправо. 5 - 8 - круговые движения туловищем влево. Повторить 4 раза. Темп средний;

7) и.п. - о.с. 1 - мах правой ногой назад, руки в стороны. 2 - и.п. 3

- 4 - то же левой ногой. Повторить 6 - 8 раз. Темп средний;

8) и.п. - ноги врозь, руки на пояс. 1 - голову наклонить вправо. 2 - не выпрямляя головы, наклонить ее назад. 3 - голову наклонить вперед. 4 - и.п. 5

- 8 - то же в другую сторону. Повторить 4 - 6 раз. Темп средний

ЗАКЛЮЧЕНИЕ

В данной работе была проанализирована предметная область, выявлены основные виды деятельности регионального модельного центра, рассмотрена его структура, определен уровень автоматизации, выбрана конфигурация ВС, спроектирована структурная схема, спланирована информационная безопасность. На основании этого были выявлены проблемы, которые призвана устранить разрабатываемая ИС с модулем.

В процессе разработки, была разработана ИС и клиент- серверное приложение. В качестве языка программирования был выбран Python за скорость написания кода на нём и обширное количество общедоступных библиотек.

Разработанная ИС позволяет автоматизировать процессы организации и упростить процесс делопроизводства. А модуль локального чата позволяет упростить и ускорить коммуникацию, имеет удобный пользовательский интерфейс, позволяет сотрудникам организации меньше тратить времени на общие сборы и не упускать важные распоряжения от директора. С модулем могут работать сотрудники разных должностей и разного уровня владения компьютером, эта возможность реализована благодаря максимально упрощенным и дружественным интерфейсом клиентской части приложения. Также в целях безопасности, в модуль встроены уведомления об ошибках, которые осведомят пользователя о неверном действии с его стороны или невозможности выполнения действия.

В итоге, работа выполнена в соответствии с техническим заданием. Разработана и спроектирована автоматизированная информационная система, основанная на локальной вычислительной сети организации « ГАУ ДПО « АмИРО» Региональный модельный центр». Разработанное приложение отвечает всем требованиям предметной области и всем нормативным документам.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ 34.602 – 89. Техническое задание на создание информационных систем - Москва: Изд- во стандартов, 1990. – 17 с.

2. ГОСТ 34.003 – 90. Термины и определения основных понятий в области автоматизированных систем– Москва: Изд- во стандартов, 1991.–32 с.

3. ГОСТ РД 50-34.698 – 90. комплекс стандартов и руководящих документов на автоматизированные системы - Москва: Изд- во стандартов, 1991. – 27 с.

4. ГОСТ 2.105 – 95. Общие требования к текстовым документам. – Москва: Изд- во стандартов, 1981. – 32 с.

5. Инструментальная среда BPWin. [Электронный ресурс]. – Режим доступа: http:// ali- ce. stup. ac. ru/ case/ caseinfo/ bpwin/ part1. html. – 10.03.2021.

6. Правила оформления дипломных и курсовых работ (проектов) [Текст] стандарт Амур. гос. ун- та / АмГУ ; АмГУ. - Благовещенск: Изд- во Амур. гос. ун- та, 2018. - 75 с.

7. Лутц М. Изучаем Python, 4-е издание. – Пер. с англ. – СПб.: Символ- Плюс, 2011. – 1280 с.

8. Свейгарт, Автоматизация рутиных задач с помощью Python: практическое руководство для начинающих. Пер. с англ. — М.: Вильямс, 2016. – 592 с.

9. Коннолли, Т. Базы данных. Проектирование, реализация и сопровождение. Теория и практика/ Т. Коннолли, К. Бегг. – Киев.: « Вильямс», 2017. – 1440 с.

10. Тидвелл, Д. Разработка пользовательских интерфейсов/ Д. Тидвелл. – СПб.: « Питер», 2011. – 480 с.

11. Проектирование информационных систем: курс лекций / А. В. Бушманов; Федеральное агентство по образованию, Амурский гос. ун-т. - Благовещенск : АмГУ, 2008 (Благовещенск : Тип. АмГУ). - 111 с.

12. Пособие по безопасной работе на персональных компьютерах [Текст] / разраб. В. К. Шумилин. - М. : НЦ ЭНАС, 2005. - 28 с.

13. Шумилин, В.К. ПЭВМ. Защита пользователя [Текст] / Шумилин В.К. - М. : Охрана труда и социальное страхование, 2001. - 214с.

14. Кардаш, Т. А. Эргономика рабочих мест служащих и инженерно- технических работников, оснащенных ПЭВМ [Текст] : учеб. пособие / Т. А. Кардаш ; АмГУ, ИФФ. - Благовещенск : Изд- во Амур. гос. ун- та, 2002. - 60 с.

15. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом ФСТЭК России № 21 от 18 февраля 2013 года);

16. Методика определения актуальных угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 14 февраля 2008г. заместителем директора ФСТЭК России);

17. Базовая модель угроз безопасности персональных данных при их обработке, в информационных системах персональных данных (утверждена 15 февраля 2008г. заместителем директора ФСТЭК России);

18. Комплексное обеспечение информационной безопасности автоматизированных систем [Электронный ресурс] : сб. учеб.- метод. материалов для направления подготовки 10.03.01 " Информационная безопасность" / АмГУ, ФМиИ ; сост. Л. А. Соловцова. - Благовещенск : Изд- во Амур. гос. ун- та, 2019. - 26 с. - Б. ц.

19. Ивановский, С. Операционная система Linux [Текст] / С. Ивановский. - 2-е изд. - М. : Познавательная книга плюс, 2001. - 512 с.

20. Бэндл, Дэвид. Защита и безопасность в сетях Linux [Текст] : производственно- практическое издание / Д. Бэндл; Пер. с англ. П. Анджан, Пер. с англ. Л. Романов. - СПб. : Питер, 2002. - 480 с.

21. Управление процессами в операционных системах Windows и Linux [Электронный ресурс] : метод. указания / сост.: Н. А. Иванов, Т. А. Федосеева. - М. : Моск. гос. строит. ун-т, 2015. - 48 с.

22. Колисниченко, Денис Николаевич. Ubuntu Linux 7.04 [Текст] : рук. пользователя / Д. Н. Колисниченко. - СПб. : Питер, 2008. - 189 с.

23. Кюнель Samba: интеграция Linux/ Unix- компьютеров в сети Windows / Кюнель, Йенц. - М.: Мн: Новое знание, 2003. - 399 с.

ПРИЛОЖЕНИЕ А

Техническое задание

1. ВВЕДЕНИЕ

1.1. Наименование программы

Локальный мессенджер для сотрудников организации « ГАУ ДПО « АмИРО» Региональный модельный центр».

1.2. Краткая характеристика области применения программы

Мессенджер предназначен для использования в локальной сети только указанной организации для быстрой связи между сотрудниками.

2. ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ

2.1. Основание для проведения разработки

Основанием для проведения разработки является выполнение курсовой работы по дисциплине « Проектирование информационных систем».

2.2. Наименование и условное обозначение темы разработки

Наименование темы разработки – « Локальный мессенджер для сотрудников организации « ГАУ ДПО « АмИРО» Региональный модельный центр»».

Условное обозначение темы разработки - « Локальный чат для сотрудников РМЦ».

3. НАЗНАЧЕНИЕ РАЗРАБОТКИ

3.1. Функциональное назначение программы

Функциональным назначением программы является обмен быстрыми сообщениями между сотрудниками внутри организации.

3.2. Эксплуатационное назначение программы

Программа должна эксплуатироваться в организации « ГАУ ДПО « АмИРО» Региональный модельный центр»».

Конечными пользователями программы должны являться все сотрудники РМЦ.

4. ТРЕБОВАНИЯ К ПРОГРАММЕ

4.1. Требования к функциональным характеристикам

4.1.1. Требования к составу выполняемых функций

Программа должна обеспечивать возможность выполнения перечисленных ниже функций:

Авторизация пользователей;

Возможность отправить сообщение в общий чат организации

4.1.2. Требования к организации входных данных

Входные данные программы должны быть организованы в виде вводимого в специальную форму текста.

4.1.3. Требования к организации выходных данных

Выходные данные программы должны быть организованы в виде сообщений от пользователей.

Вся история сообщений должна храниться на сервере в локальной сети, который находиться в защищенном от несанкционированного доступа месте.

4.1.4. Требования к временным характеристикам

Обработка ввода информации и показа уведомления не должны превышать 1 сек.

4.2. Требования к надежности

4.2.1. Требования к обеспечению надежного (устойчивого) функционирования программы

Надежное (устойчивое) функционирование программы должно быть обеспечено выполнением совокупности организационно- технических мероприятий:

а) организацией бесперебойного питания технических средств;

б) выполнением рекомендаций Министерства труда и социального развития РФ, изложенных в Постановлении от 23 июля 1998 г. « Об утверждении межотраслевых типовых норм времени на работы по сервисному обслуживанию ПЭВМ и оргтехники и сопровождению программных средств»;

в) выполнением требований ГОСТ 51188–98. Защита информации. Испытания программных средств на наличие компьютерных вирусов;

Обеспечиваются стороной- заказчиком.

4.2.2. Время восстановления после отказа

Время восстановления после отказа, вызванного сбоем электропитания технических средств (иными внешними факторами), не фатальным сбоем (не крахом) операционной системы, не должно превышать времени, необходимого на перезагрузку операционной системы и запуск программы, при условии соблюдения условий эксплуатации технических и программных средств.

Время восстановления после отказа, вызванного неисправностью технических средств, фатальным сбоем (крахом) операционной системы, не должно превышать времени, требуемого на устранение неисправностей технических средств и переустановки программных средств.

Обеспечивается копиями (обеспечивается программой) необходимой информации и хранении дистрибутивов на отдельном компьютере (обеспечивается стороной- заказчиком).

4.2.3. Отказы из- за некорректных действий оператора

Отказы программы возможны вследствие некорректных действий оператора (пользователя) при взаимодействии с операционной системой. Во избежание возникновения отказов программы по указанной выше причине следует обеспечить работу конечного пользователя без предоставления ему административных привилегий.

4.3. Условия эксплуатации

4.3.1. Климатические условия эксплуатации

Климатические условия эксплуатации, при которых должны обеспечиваться заданные характеристики, должны удовлетворять требованиям, предъявляемым к техническим средствам в части условий их эксплуатации.

4.3.2. Требования к видам обслуживания

См. Требования к обеспечению надежного (устойчивого) функционирования программы.

4.3.3. Требования к численности и квалификации персонала

Минимальное количество персонала, требуемого для работы программы, должно составлять не менее 2 штатных единиц - системный администратор и конечный пользователь программы - оператор.

Системный администратор должен иметь минимум среднее техническое образование.

В перечень задач, выполняемых системным программистом, должны входить:

а) задача поддержания работоспособности технических средств;

б) задачи установки (инсталляции) и поддержания работоспособности системных программных средств - операционной системы;

в) задача установки (инсталляции) программы.

Конечный пользователь программы (оператор) должен обладать практическими навыками работы с графическим пользовательским интерфейсом операционной системы.

Персонал должен быть аттестован минимум на II квалификационную группу по электробезопасности (для работы с конторским оборудованием).

4.4. Требования к составу и параметрам технических средств

В состав технических средств должен входить IBM- совместимый персональный компьютер (ПЭВМ), включающий в себя:

1) процессор Pentium – 4 (AMD Athlon-64 X2) с тактовой частотой, 1.2 ГГц, не менее;

2) оперативную память объемом, 2 ГБ, не менее;

3) жесткий диск объемом 20 Гб, и выше;

4) манипулятор типа « мышь»;

5) наличие 2 COM- портов;

6) клавиатуру.

А также необходимы одна серверная платформа в качестве хранителя истории сообщений и обрабатывающий станции.

В случае работы системы в сети все компьютеры должны быть подобны. Так же необходимы кабеля для создания сети, сетевые карты на каждом компьютере и маршрутизатор.

При предоставлении возможности поступления информации через сеть Интернет, один из компьютеров в сети, не являющийся сервером, должен иметь модем.

4.5. Требования к информационной и программной совместимости

4.5.1. Требования к информационным структурам и методам решения

Пользовательский интерфейс должен быть интуитивно понятным и содержать подсказки.

4.5.2. Требования к исходным кодам и языкам программирования

Исходные коды программы должны быть реализованы на языке Python. В качестве интегрированной среды разработки программы должна быть использована среда PyCharm community.

4.5.3. Требования к программным средствам, используемым программой

Системные программные средства, используемые программой, должны быть представлены локализованной версией операционной системы Windows.

Основой для системы должна стать серверная часть, в которой будет храниться вся история сообщений и обрабатываться запросы на отправку новых сообщений.

Подсистема администрирования.

Подсистема администрирования предназначена для управления настроек программного продукта. Управление осуществляется администратором. Управление должно учитывать настройку следующих параметров:

1. сетевые параметры,
2. системные параметры.

4.5.4. Требования к защите информации и программ

В Системе должен быть обеспечен надлежащий уровень защиты информации в соответствии с законом о защите персональной информации и программного комплекса в целом от несанкционированного доступа - “ Об информации, информатизации и защите информации” РФ N 24- ФЗ от 20.02.95.

4.6. Специальные требования

Программа должна обеспечивать взаимодействие с пользователем (оператором) посредством графического пользовательского интерфейса, разработанного согласно рекомендациям компании- производителя операционной системы. Программа должна обеспечивать высокую защиту данных и удобный и быстрый просмотр необходимой информации посредством отчетов.

5. ТРЕБОВАНИЯ К ПРОГРАММНОЙ ДОКУМЕНТАЦИИ

5.1. Предварительный состав программной документации

Состав программной документации должен включать в себя:

1) техническое задание;
2) спецификация;
3) текст программы;
4) описание программы;
5) программу и методики испытаний;
6) пояснительная записка;
7) ведомость эксплуатационных документов;
8) формуляр;
9) описание применения;
10) руководство системного администратора;
11) руководство оператора

5.2. Специальные требования к программной документации

Специальные требования к программной документации не предъявляются.

6. ТЕХНИКО- ЭКОНОМИЧЕСКИЕ ПОКАЗАТЕЛИ

6.1. Ориентировочная экономическая эффективность

Ориентировочная экономическая эффективность не рассчитываются.

6.2. Предполагаемая годовая потребность

Предполагаемое число использования программы в год – круглосуточная работа программы на одном рабочем месте. Возможность работы в сети в таком же режиме.

7. СТАДИИ И ЭТАПЫ РАЗРАБОТКИ

7.1. Стадии разработки

Разработка должна быть проведена в три стадии:

1) разработка технического задания;
2) рабочее проектирование;
3) внедрение.

7.2. Этапы разработки

На стадии разработки технического задания должен быть выполнен этап разработки, согласования и утверждения настоящего технического задания.

На стадии рабочего проектирования должны быть выполнены перечисленные ниже этапы работ:

1) разработка программы;
2) разработка программной документации;
3) испытания программы.

На стадии внедрения должен быть выполнен этап разработки - подготовка и передача программы.

7.3. Содержание работ по этапам

На этапе разработки технического задания должны быть выполнены перечисленные ниже работы:

1) постановка задачи;
2) определение и уточнение требований к техническим средствам;
3) определение требований к программе;

4) определение стадий, этапов и сроков разработки программы и документации на неё;

5) выбор языков программирования;

6) согласование и утверждение технического задания.

На этапе разработки программы должна быть выполнена работа по программированию и отладке программы.

На этапе разработки программной документации должна быть выполнена разработка программных документов в соответствии с требованиями ГОСТ 19.101–77 и требованием п. « Предварительный состав программной документации» настоящего технического задания.

На этапе испытаний программы должны быть выполнены перечисленные ниже виды работ:

1) разработка, согласование и утверждение программы и методики испытаний;

2) проведение приемо- сдаточных испытаний;

3) корректировка программы и программной документации по результатам испытаний.

На этапе подготовки и передачи программы должна быть выполнена подготовка и передача программы и программной документации в эксплуатацию.

7.4. Исполнители

Руководитель разработки

Преподаватель Бушманов А.В.

Исполнитель

Студент группы 755- об Бурдуковский Д.В.

ПРИЛОЖЕНИЕ Б

Экз.№__

УТВЕРЖДАЮ

Директор

_____ С.А. Голубева

«___» _____ 20___ года

МОДЕЛЬ
угроз и модель нарушителей безопасности информационной системы персональных данных « ИСПДн РМЦ»

г. Благовещенск

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ

АВС – антивирусные средства
АС – автоматизированная система
АРМ – автоматизированное рабочее место
БД – база данных
ВТСС – вспомогательные технические средства и системы
ИКХ – информация конфиденциального характера
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
ЛВС – локальная вычислительная сеть
НСД – несанкционированный доступ к информации
МЭ – межсетевой экран
ОС – операционная система
ПДн – персональные данные
ПМВ – программно- математическое воздействие
ПО – программное обеспечение
ППО – прикладное программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СВТ – средства вычислительной техники
СЗИ – средство защиты информации
СКЗИ – средство криптографической защиты информации
СЗПДн – система защиты персональных данных
СОВ – система обнаружения вторжений
СФ – среда функционирования
ТКУИ – технические каналы утечки информации
УБПДн – угрозы безопасности персональных данных
ФСТЭК России – Федеральная служба по техническому и экспортному контролю

Термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищенности персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

Доступ в операционную среду компьютера (информационной системы персональных данных) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально- распределенное программное (программно- аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлеченных из такой системы, считается осуществленной без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

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

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки ПДн (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно- цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес,

семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Политика « чистого стола» – комплекс организационных мероприятий, контролирующих отсутствие записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы персональных данных и (или) блокировать аппаратные средства.

Программное (программно- математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определенному кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким- либо иным способом.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Специальные категории персональных данных – персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья и интимной жизни субъекта персональных данных.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

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

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Учреждение – учреждения здравоохранения, социальной сферы, труда и занятости.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность

информации в условиях случайного и/ или преднамеренного искажения (разрушения).

1. Введение

Настоящий документ подготовлен в рамках выполнения работ по построению системы защиты персональных данных (далее – СЗПДн), не содержащей сведений, составляющих государственную тайну, информационной системы персональных данных « ИСПДн РМЦ» (далее – ИСПДн, ИСПДн « ИС РМЦ»).

Настоящий документ содержит модель угроз и модель нарушителей безопасности персональных данных для ИСПДн (далее – модель угроз).

Разработка модели угроз является необходимым условием формирования обоснованных требований к обеспечению безопасности информации ИСПДн и проектирования СЗПДн ИСПДн.

Модель угроз – документ, использующийся для:

- анализа защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн;
- разработки системы защиты ПДн, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты ПДн, предусмотренных для соответствующего класса ИСПДн;
- проведения мероприятий, направленных на предотвращение несанкционированного доступа к ПДн и (или) передачи их лицам, не имеющим права доступа к такой информации;
- недопущения воздействия на технические средства ИСПДн, в результате которого может быть нарушено их функционирование;
- контроля обеспечения уровня защищенности персональных данных.

В модели угроз представлено описание структуры ИСПДн, состава и режима обработки ПДн, классификацию потенциальных нарушителей, оценку исходного уровня защищенности, анализ угроз безопасности персональных данных.

Анализ УБПДн включает:

- описание угроз;
- оценку вероятности возникновения угроз;
- оценку реализуемости угроз;
- оценку опасности угроз;
- определение актуальности угроз.

Модель угроз для ИСПДн разрабатывается в соответствии со следующими нормативными и методическими документами:

- Федеральный закон от 27.07.2006 № 149- ФЗ « Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152- ФЗ «О персональных данных»;

- Постановлением Правительства Российской Федерации от 01.11.2012 № 1119 « Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
- Приказ ФСТЭК России от 18.02.2013 № 21 « Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена Заместителем директора ФСТЭК России 15.02.2008;
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утверждена заместителем директора ФСТЭК России 14.02.2008;
- Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, утверждены приказом ФСБ России от 10.07.2014 № 378;
- Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности, утверждены руководством 8 Центра ФСБ России 31.03.2015 № 149/7/2/6-432;

В процессе развития ИСПДн предполагается конкретизировать и пересматривать модель угроз для ИСПДн.

Модель угроз может быть пересмотрена:

- по решению оператора на основе периодически проводимых им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или) изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

При разработке модели угроз для ИСПДн учитывается:

1. В ИСПДн одновременно обрабатываются данные от 1000 до 100000 субъектов персональных данных;
2. В ИСПДн не предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных

решений, порождающих юридические последствия в отношении субъекта персональных (юридически значимым документом является « бумажная» история болезни, по которой принимаются решения).

2. НАЗНАЧЕНИЕ, СТРУКТУРА И ОСНОВНЫЕ ХАРАКТЕРИСТИКИИ ИСПДн

ИСПДн « ИСПДн РМЦ» предназначена для проведения внутреннего документооборота.

ИСПДн позволяет обмениваться документами.

Рассматриваемая ИСПДн имеет одноточечное подключение к сетям общего пользования и (или) международного обмена. Подключение к сетям общего пользования и (или) международного обмена используется для подключения к ИС Навигатор для её администрирования.

Для защиты персональных данных при передаче по сетям общего пользования и (или) международного обмена используются СКЗИ.

Все компоненты ИСПДн находятся внутри контролируемой зоны. Доступ в контролируемую зону регламентирован внутренними локальными актами образовательной организации.

Обработка персональных данных в ИСПДн ведется в многопользовательском режиме с разгрониченными полномочиями допущенных пользователей в рамках своих служебных обязанностей.

Режим обработки предусматривает следующие действия с персональными данными: сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, предоставление (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Все технические средства находятся в пределах КЗ на территории Российской Федерации.

Основные параметры ИСПДн приведены в Таблице 1.

Таблица 1. Параметры ИСПДн.

Заданные характеристики безопасности персональных данных	Информационная система обрабатывает ПДн **третьего уровня защищенности**
Структура информационной системы	Локальная сеть с выходом в сеть Интернет посредством МЭ
Подключение информационной системы к сетям общего пользования и (или) сетям международного информационного обмена	Имеется
Режим обработки персональных данных	Многопользовательская ИС

Режим разграничения прав доступа пользователей	Разграниченные полномочия
Местонахождение технических средств информационной системы	Все технические средства находятся в пределах КЗ на территории Российской Федерации
Дополнительная информация	

В ИСПД обрабатываются следующие категории ПДн:

- Фамилия, Имя, Отчество
- Дата рождения
- Пол
- СНИЛС
- прочая информация о субъекте персональных данных.

В ИСПДн для обрабатываемых персональных данных необходимо обеспечивать следующие характеристики безопасности: конфиденциальность, целостность, доступность.

В ходе анализа исходных данных в соответствии с приказом ФСТЭК России от 18.02.2013 № 21 « Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» определен Актом третий уровень защищённости ПДн в ИСПДн.

Для функционирования прикладных программ в состав ИСПДн входит следующее оборудование: персональный компьютер, USB накопители, коммутаторы, маршрутизаторы и прочее сетевое оборудование.

При входе в систему и выдаче запросов на доступ проводится аутентификация пользователей ИСПДн. ИСПДн располагает необходимыми данными для идентификации, аутентификации, а также препятствует несанкционированному доступу к ресурсам.

Все пользователи ИСПДн имеют собственные роли. Список типовых ролей представлен в виде матрицы доступа в таблице 2.

Таблица 2. Матрица доступа.

Группа	**Уровень доступа к ПДн**	**Разрешенные действия**
Администратор безопасности	Обладает полной информацией о системном и прикладном программном обеспечении ИСПДн. Обладает полной информацией о технических средствах и конфигурации ИСПДн. Имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн. Имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов ИСПДн. Обладает правами конфигурирования и административной настройки технических средств ИСПДн.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение
Пользователи (операторы) ИСПДн с правами записи	Обладает только необходимыми атрибутами и правами, обеспечивающими доступ только к необходимым ПДн для выполнения непосредственных обязанностей.	- сбор - систематизация - накопление - хранение - уточнение - использование - уничтожение

Совместно с техническими и программными средствами обработки персональных данных в ИСПДн штатно функционируют СКЗИ, образовывая таким образом среду функционирования СКЗИ. Технические

и программные средства обработки персональных данных способны повлиять на выполнение предъявляемых к СКЗИ требований.

3. МОДЕЛЬ ВЕРОЯТНОГО НАРУШИТЕЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Описание возможных нарушителей

По признаку принадлежности к ИСПДн все нарушители делятся на две группы:

- внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД.
- внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИСПД;

Возможности внутреннего нарушителя существенным образом зависят от действующих в пределах контролируемой зоны ограничительных факторов, из которых основным является реализация комплекса организационно- технических мер, в том числе по подбору, расстановке и обеспечению высокой профессиональной подготовки кадров, допуску физических лиц внутрь контролируемой зоны и контролю за порядком проведения работ, направленных на предотвращение и пресечение несанкционированных действий.

Исходя из особенностей функционирования ИСПДн, допущенные к ней физические лица, имеют разграниченные полномочия на доступ к информационным, программным, аппаратным и другим ресурсам ИСПДн в соответствии с принятой политикой информационной безопасности (правилами). К внутренним нарушителям могут относиться:

- администраторы ИСПДн (категория I), имеющие средний потенциал;
- пользователи ИСПДн (категория II), имеющие низкий потенциал;
- сотрудники, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы ИСПДн, но не имеющие права доступа к ресурсам (категория III), имеющие низкий потенциал;
- обслуживающий персонал (охрана, работники инженерно-технических служб и т.д.) (категория IV), имеющие низкий потенциал;
- уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн (категория V), имеющие средний потенциал.

Потенциал нарушителя определяется компетентностью, ресурсами и мотивацией, требуемыми для реализации угроз безопасности информации

в информационной системе с заданными структурно- функциональными характеристиками и особенностями функционирования.

Нарушители с низким потенциалом могут для реализации атак использовать информацию только из общедоступных источников. К нарушителям с низким потенциалом относятся любые внешние нарушители, а также внутренний персонал и пользователи ИСПДн.

Нарушители со средним потенциалом имеют возможность проводить анализ кода прикладного программного обеспечения, самостоятельно находить в нем уязвимости и использовать их. К таким нарушителям относятся администраторы системы и разработчики программного обеспечения.

На лиц I категории возложены задачи по администрированию программно- аппаратных средств и баз данных ИСПДн для интеграции и обеспечения взаимодействия различных подсистем, входящих в состав ИСПДн. Администраторы потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них административными полномочиями.

Эти лица хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Кроме того, предполагается, что эти лица могли бы располагать специализированным оборудованием.

На лиц II категории возложены задачи по использованию программно- аппаратных средств и баз данных ИСПДн. Пользователи потенциально могут реализовывать угрозы ИБ используя возможности по непосредственному доступу к защищаемой информации, обрабатываемой и хранимой в ИСПДн, а также к техническим и программным средствам ИСПДн, включая средства защиты, используемые в конкретных АС, в соответствии с установленными для них полномочиями.

К лицам категорий I и II ввиду их исключительной роли в ИСПДн должен применяться комплекс особых организационных мер по их

подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Предполагается, что в число лиц категорий I и II будут включаться только доверенные лица и поэтому указанные лица исключаются из числа вероятных нарушителей.

Предполагается, что лица категорий III- VII относятся к вероятным нарушителям.

Предполагается, что возможность сговора внутренних нарушителей маловероятна ввиду принятых организационных и контролирующих мер.

В качестве внешнего нарушителя информационной безопасности рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

Предполагается, что внешний нарушитель не может воздействовать на защищаемую информацию по техническим каналам утечки, так как объем информации, хранимой и обрабатываемой в ИСПДн, является недостаточным для возможной мотивации внешнего нарушителя к осуществлению действий, направленных утечку информации по техническим каналам утечки.

К внешним нарушителям могут относиться:

- бывшие сотрудники – администраторы или пользователи ИСПД (категория VI), имеющие низкий потенциал;
- посторонние лица, пытающиеся получить доступ к ПДн в инициативном порядке (категория VII), имеющие низкий потенциал;

Лица категории VI хорошо знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, а также с применяемыми принципами и концепциями безопасности. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может быть, как частью штатных средств, так и может относиться к легко получаемому (например, программное обеспечение, полученное из общедоступных внешних источников).

Лица категории VII могут быть знакомы с основными алгоритмами, протоколами, реализуемыми и используемыми в конкретных подсистемах и ИСПДн в целом, но не знакомы с применяемыми принципами и концепциями безопасности на объекте ИСПДн. Предполагается, что они могли бы использовать стандартное оборудование либо для идентификации уязвимостей, либо для реализации угроз ИБ. Данное оборудование может относиться к легко получаемому (например,

программное обеспечение, полученное из общедоступных внешних источников).

Лица категорий VI и VII потенциально могут реализовывать угрозы ИБ, используя возможности по несанкционированному доступу к защищаемой информации по каналам связи, обрабатываемой и хранимой в ИСПДн.

Предполагается, что лица категорий VI и VII относятся к вероятным нарушителям.

В связи с использованием средств СКЗИ для обеспечения безопасности персональных данных при передаче по каналам связи, ИСПДн имеет внешние источники атак не имеющие возможности доступа к объектам защиты, однако способные осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны.

3.2. Предположения об имеющейся у нарушителя информации об объектах реализации угроз.

В качестве основных уровней знаний нарушителей об АС можно выделить следующие:

- информации о назначении и общих характеристиках ИСПДн;
- информация, полученная из эксплуатационной документации;
- информация, дополняющая эксплуатационную информацию об ИСПДн (например, сведения из проектной документации ИСПДн).

В частности, нарушитель может иметь:

- данные об организации работы, структуре и используемых технических, программных и программно- технических средствах ИСПДн;
- сведения об информационных ресурсах ИСПДн: порядок и правила создания, хранения и передачи информации, структура и свойства информационных потоков;
- данные об уязвимостях, включая данные о недокументированных (недекларированных) возможностях технических, программных и программно- технических средств ИСПДн;
- данные о реализованных в СЗИ принципах и алгоритмах;
- исходные тексты программного обеспечения ИСПДн;
- сведения о возможных каналах реализации угроз;
- информацию о способах реализации угроз.

Предполагается, что лица категорий III - VII не владеют парольной и аутентифицирующей информацией, используемой в ИС.

Предполагается, что лица категорий V – VI обладают чувствительной информацией об ИСПДн и функционально ориентированных АС, включая информацию об уязвимостях технических и программных средств ИСПДн.

Организационными мерами предполагается исключить доступ лиц категории V к техническим и программным средствам ИСПД в момент обработки с использованием этих средств защищаемой информации.

Предполагается полностью исключить доступ лиц категорий VI – VII к техническим и программным средствам ИСПДн.

Таким образом, наиболее информированными об АС являются лица категорий V – VI.

Степень информированности нарушителя зависит от многих факторов, включая реализованные конкретные организационные меры и компетенцию нарушителей. Поэтому объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно.

В связи с изложенным, с целью создания необходимых условий безопасности персональных данных предполагается, что вероятные нарушители обладают всей информацией, необходимой для подготовки и реализации угроз, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации. К такой информации, например, относится парольная, аутентифицирующая и ключевая информация.

3.3. Предположения об имеющихся у нарушителя средствах реализации угроз

Предполагается, что нарушитель имеет:

- аппаратные компоненты СЗПДн и СФ СЗПДн;
- доступные в свободной продаже технические средства и программное обеспечение.

Предполагается что содержание и объем персональных данных, находящихся в ИСПДн не достаточны для мотивации применения нарушителем специально разработанных технических средства и программного обеспечения.

Внутренний нарушитель может использовать штатные средства.

Состав имеющихся у нарушителя средств, которые он может использовать для реализации угроз ИБ, а также возможности по их применению зависят от многих факторов, включая реализованные на объекте ИСПДн конкретные организационные меры, финансовые возможности и компетенцию нарушителей. Поэтому объективно оценить состав имеющихся у нарушителя средств реализации угроз в общем случае практически невозможно.

Поэтому, для определения актуальных угроз и создания СЗПДн предполагается, что вероятный нарушитель имеет все необходимые для

реализации угроз средства, доступные в свободной продаже, возможности которых не превосходят возможности аналогичных средств реализации угроз на информацию, содержащую сведения, составляющие государственную тайну, и технические и программные средства, обрабатывающие эту информацию.

Вместе с тем предполагается, что нарушитель не имеет:

- средств перехвата в технических каналах утечки;
- средств воздействия через сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- средств воздействия на источники и через цепи питания;
- средств воздействия через цепи заземления;
- средств активного воздействия на технические средства (средств облучения).

Предполагается, что наиболее совершенными средствами реализации угроз обладают лица категории V- VII.

3.4. Описание объектов и целей реализации угроз информационной безопасности

Основными информационными ресурсами, обрабатываемыми в ИСПД являются следующие:

1. Целевая информация:

- служебная информация;
- персональные данные;
- сведения из базы данных ИСПДн.

2. Технологическая информация:

- защищаемая управляющая информация (конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.);
- защищаемая технологическая информация средств доступа к системам управления ИСПДн (аутентификационная информация и др.);
- информационные ресурсы ИСПДн на съемных носителях информации (бумажные, магнитные, оптические, электронные и пр.), содержащие защищаемую технологическую информацию системы управления ресурсами ИСПДн (программное обеспечение, конфигурационные файлы, таблицы маршрутизации, настройки системы защиты и пр.) или средств доступа к этим системам управления (аутентификационная информация и др.);
- информация о СЗПДн, их структуре, принципах и технических решениях защиты;
- информационные ресурсы ИСПДн (базы данных и файлы), содержащие информацию о информационно- телекоммуникационных системах, о служебном, телефонном, факсимильном, диспетчерском трафике, о событиях, произошедших с управляемыми объектами, о планах

обеспечения бесперебойной работы и процедурах перехода к управлению в аварийных режимах.

3. Программное обеспечение:

- программные информационные ресурсы ИСПДн, содержащие общее и специальное программное обеспечение, резервные копии общесистемного программного обеспечения, инструментальные средства и утилиты систем управления ресурсами ИСПДн, чувствительные по отношению к случайным и несанкционированным воздействиям, программное обеспечение средств защиты.

Предполагается, что не являются объектами реализации угроз:

- технические каналы утечки информации;
- сигнальные цепи (информационные и управляющие интерфейсы СВТ);
- источники и цепи электропитания;
- цепи заземления.

Целью реализации угроз является нарушение определенных для объекта реализации угроз характеристик безопасности (таких как, конфиденциальность, целостность, доступность) или создание условий для нарушения характеристик безопасности объекта реализации угроз.

3.5. Описание каналов реализации угроз информационной безопасности

Возможными каналами реализации угроз информационной безопасности являются:

- каналы доступа, образованные с использованием штатных средств ИСПДн;
- каналы доступа, образованные с использованием специально разработанных технических средств и программного обеспечения.

Предполагается, что не являются каналами реализации угроз:

- технические каналы утечки;
- сигнальные цепи;
- источники и цепи электропитания;
- цепи заземления;
- каналы активного воздействия на технические средства с помощью облучения.

3.6. Основные способы реализации угроз информационной безопасности

При определении основных способов реализации угроз информационной безопасности ресурсов ИСПДн, учитывались необходимость обеспечения информационной безопасности на всех этапах

жизненного цикла ИСПДн, компонентов, условий функционирования ИСПДн, а также - предположения о вероятных нарушителях.

Возможны следующие способы реализации угроз информационной безопасности ИСПДн:

1) несанкционированный доступ к защищаемой информации с использованием штатных средств ИСПДн и недостатков механизмов разграничения доступа;

2) негативные воздействия на программно- технические компоненты ИСПДн вследствие внедрения компьютерных вирусов и другого вредоносного программного обеспечения;

3) маскировка под администратора ИСПДн, уполномоченного на необходимый нарушителю вид доступа с использованием штатных средств, предоставляемых ИСПДн;

4) осуществление прямого хищения (утраты) элементов ИСПДн, носителей информации и производственных отходов (распечаток, списанных носителей);

5) компрометация технологической (аутентификационной) информации путем визуального несанкционированного просмотра и подбора с использованием штатных средств, предоставляемых ИСПДн;

6) методы социальной инженерии для получения сведений об ИСПДн, способствующих созданию благоприятных условий для применения других методов;

7) использование оставленных без присмотра незаблокированных средств администрирования ИСПДн и АРМ;

8) сбои и отказы программно- технических компонентов ИСПДн;

9) внесение неисправностей, уничтожение технических и программно- технических компонентов ИСПДн путем непосредственного физического воздействия;

10) осуществление несанкционированного доступа к информации при ее передаче.

4. ИСХОДНЫЙ УРОВЕНЬ ЗАЩИЩЕННОСТИ ИСПДН

Под общим уровнем защищенности понимается обобщенный показатель, зависящий от технических и эксплуатационных характеристик ИСПДн (Y_1) в соответствии с Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утверждена заместителем директора ФСТЭК России 14 февраля 2008 г.).

В таблице представлены характеристики уровня исходной защищенности для ИСПДн.

Таблица 3. Исходный уровень защищенности

№ п/п	Технические и эксплуатационные характеристики	Уровень защищенности
1.	По территориальному размещению *(локальная ИСПДн, развернутая в пределах одного здания)*	Высокий
2.	По наличию соединения с сетями общего пользования *(ИСПДн, имеющая одноточечный выход в сеть общего пользования*)	Средний
3.	По встроенным (легальным) операциям с записями баз персональных данных *(модификация, передача)*	Низкий
4.	По разграничению доступа к персональным данным *(ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн)*	Средний
5.	По наличию соединений с другими базами ПДн иных ИСПДн *(ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн)*	Высокий
6.	По уровню (обезличивания) ПДн *(ИСПДн, в которой предоставляемые пользователю данные не являются обезличенными (т.е.*	Низкий

	присутствует информация, позволяющая идентифицировать субъекта ПДн)	
7.	По объему ПДн, которые предоставляются сторонним пользователям ИСПДн без предварительной обработки *(ИСПДн, предоставляющая часть ПДн)*	Средний

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

Показатель исходной защищенности Y_1 =5.

5. ВЕРОЯТНОСТЬ РЕАЛИЗАЦИИ УБПДН

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

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

- маловероятно - отсутствуют объективные предпосылки для осуществления угрозы (Y2 = 0);
- низкая вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (Y2 = 2);
- средняя вероятность - объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны (Y2 = 5);
- высокая вероятность - объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты (Y2 = 10).

Выделим следующие угрозы при обработке персональных данных в ИСПДн:

5.1. Угрозы утечки информации по техническим каналам

5.1.1. Угрозы утечки акустической (речевой) информации

Возникновение угроз утечки акустической (речевой) информации, содержащейся непосредственно в произносимой речи пользователя ИСПДн, при обработке ПДн в ИСПДн, возможно при наличии функций голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн.

В ИСПДн функции голосового ввода ПДн или функции воспроизведения ПДн акустическими средствами отсутствуют.

Вероятность реализации угрозы – маловероятна.

5.1.2. Угрозы утечки видовой информации

Реализация угрозы утечки видовой информации возможна за счет просмотра информации с помощью оптических (оптико- электронных) средств с экранов дисплеев и других средств отображения средств вычислительной техники, информационно- вычислительных комплексов,

технических средств обработки графической, видео и буквенно- цифровой информации, входящих в состав ИСПДн.

Введен контроль доступа в контролируемую зону. Расположение АРМ ИСПДн на объекте информатизации исключает визуальный просмотр посторонними лицами информации на мониторе и при выводе информации на твердую копию при распечатке.

Вероятность реализации угрозы – маловероятна.

5.1.3. Угрозы утечки информации по каналам ПЭМИН

Угрозы утечки информации по каналу ПЭМИН маловероятны, ввиду недостаточной мотивации для применения дорогостоящих средств разведки в отношении информации обрабатываемой в ИСПДн.

5.2. Угрозы несанкционированного доступа к информации

Реализация угроз НСД к информации может приводить к следующим видам нарушения ее безопасности:

- нарушению конфиденциальности (копирование, неправомерное распространение);
- нарушению целостности (уничтожение, изменение);
- нарушению доступности (блокирование).

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

5.2.1.1. Кража ПЭВМ.

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

Введен круглосуточный контроль доступа в контролируемую зону, который осуществляется охраной, двери, закрываются на замок, вынос компьютерный техники за пределы здания возможен только по специальным пропускам.

Вероятность реализации угрозы – маловероятна.

5.2.1.2. Кража носителей информации

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

Введен контроль доступа в контролируемую зону, двери закрываются на замок, ведется учет носителей.

Вероятность реализации угрозы – маловероятна.

5.2.1.3. Кража ключей и атрибутов доступа

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

Введен контроль доступа в контролируемую зону, двери закрываются на замок, организовано хранение ключей и паролей в сейфе и введена политика «чистого стола». Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

5.2.1.4. Кражи, модификации, уничтожения информации

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

Введен контроль доступа в контролируемую зону, двери закрываются на замок. Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

5.2.1.5. Вывод из строя узлов ПЭВМ, каналов связи

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

Введен контроль доступа в контролируемую зону, двери закрываются на замок.

Вероятность реализации угрозы – маловероятна.

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

В техническое обслуживание ПЭВМ осуществляется собственными работниками. Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

5.2.1.7. Несанкционированное отключение средств защиты

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

В здании организации введен контроль доступа в контролируемую зону, двери закрываются на замок, пользователи ИСПДн проинструктированы о работе с ПДн. Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

5.2.2. 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).

5.2.2.1. Действия вредоносных программ (вирусов).

Программно- математическое воздействие - это воздействие с помощью вредоносных программ. Программой с потенциально опасными последствиями или вредоносной программой (вирусом) называют некоторую самостоятельную программу (набор инструкций), которая способна выполнять любое непустое подмножество следующих функций:

- скрывать признаки своего присутствия в программной среде компьютера;
- обладать способностью к самодублированию, ассоциированию себя с другими программами и (или) переносу своих фрагментов в иные области оперативной или внешней памяти;
- разрушать (искажать произвольным образом) код программ в оперативной памяти;
- выполнять без инициирования со стороны пользователя (пользовательской программы в штатном режиме ее выполнения) деструктивные функции (копирования, уничтожения, блокирования и т.п.);
- сохранять фрагменты информации из оперативной памяти в некоторых областях внешней памяти прямого доступа (локальных или удаленных);
- искажать произвольным образом, блокировать и (или) подменять вы- водимый во внешнюю память или в канал связи массив информации, образовавшийся в результате работы прикладных программ, или уже находящиеся во внешней памяти массивы данных.

На всех элементах ИСПДн установлена антивирусная защита, пользователи проинструктированы о мерах предотвращения вирусного заражения.

Вероятность реализации угрозы – низкая вероятность.

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

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

Для обработки ПДн и в качестве среды функционирования применяются только лицензионные программные продукты, выполняются все рекомендации по локализации выявленных в ПО уязвимостей.

Вероятность реализации угрозы – маловероятна.

5.2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей

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

Все пользователи проинструктированы о политике установки ПО и осуществляется контроль.

Вероятность реализации угрозы – средняя вероятность.

5.2.3. Угрозы непреднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн и СЗПДн в ее составе из- за сбоев в программном обеспечении, а также от угроз неантропогенного (сбоев аппаратуры из- за ненадежности элементов, сбоев электропитания) **и стихийного** (ударов молний, пожаров, наводнений и т.п.) **характера.**

5.2.3.1. Утрата ключей и атрибутов доступа

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

Введена парольная политика, предусматривающая требуемую сложность пароля, пользователи проинструктированы о парольной

политике и о действиях в случаях утраты или компрометации паролей. Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

5.2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками

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

Вероятность реализации угрозы – высокая вероятность.

5.2.3.3. Непреднамеренное отключение средств защиты

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

Введен контроль доступа в контролируемую зону, двери закрываются на замок, осуществляется разграничение доступа к настройкам режимов средств защиты, пользователи проинструктированы о работе с ИСПДн. Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

5.2.3.4. Выход из строя аппаратно- программных средств

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

Осуществляется резервирование ключевых элементов ИСПДн.

Вероятность реализации угрозы – средняя вероятность.

5.2.3.5. Сбой системы электроснабжения

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

Ко всем ключевым элементам ИСПДн подключены источники бесперебойного питания.

Вероятность реализации угрозы – маловероятна.

5.2.3.6. Стихийное бедствие

Угроза осуществляется вследствие несоблюдения мер пожарной безопасности.

Установлена пожарная сигнализация, пользователи проинструктированы о действиях в случае возникновения внештатных ситуаций.

Вероятность реализации угрозы – маловероятна.

5.2.4. Угрозы преднамеренных действий внутренних нарушителей

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

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

Введен контроль доступа в контролируемую зону, двери закрываются на замок. Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

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

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

Пользователи осведомлены о порядке работы с персональными данными, а также подписали Соглашение о неразглашении.

Вероятность реализации угрозы – маловероятна.

5.2.5. Угрозы несанкционированного доступа по каналам связи

В соответствии с « Типовой моделью угроз безопасности персональных данных, обрабатываемых в распределенных ИСПДн, имеющих подключение к сетям общего пользования и (или) международного информационного обмена» (п. 6.6. Базовой модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденной заместителем директора ФСТЭК России 15.02.2008), для ИСПДн можно рассматривать следующие

угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:

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

5.2.5.1. Угроза « Анализ сетевого трафика»

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

- изучает логику работы ИСПДн - то есть стремится получить однозначное соответствие событий, происходящих в системе, и команд, пересылаемых при этом хостами, в момент появления данных событий. В дальнейшем это позволяет злоумышленнику на основе задания соответствующих команд получить, например, привилегированные права на действия в системе или расширить свои полномочия в ней;
- перехватывает поток передаваемых данных, которыми обмениваются компоненты сетевой операционной системы, для извлечения конфиденциальной или идентификационной информации (например, статических паролей пользователей для доступа к удаленным хостам по протоколам FTP и TELNET, не предусматривающих шифрование), ее подмены, модификации и т.п.

На границе сети используется сертифицированный межсетевой экран. ИСПДн осуществляет межсетевое взаимодействие с использованием СКЗИ.

Перехват за переделами контролируемой зоны.

Вероятность реализации угрозы – низкая вероятность.

Перехват в пределах контролируемой зоны внешними нарушителями

Вероятность реализации угрозы – маловероятна.

Перехват в пределах контролируемой зоны внутренними нарушителями.

Вероятность реализации угрозы – маловероятна.

5.2.5.2. Угроза « сканирование сети»

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

На границе сети используется сертифицированный межсетевой экран. ИСПДн осуществляет межсетевое взаимодействие с использованием СКЗИ.

Вероятность реализации угрозы – средняя вероятность.

5.2.5.3. Угроза выявления паролей

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

Применяются стойкие пароли. Используется средство защиты от НСД прошедшее оценку соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации.

Вероятность реализации угрозы – маловероятна.

5.2.5.4. Угрозы навязывание ложного маршрута сети

Данная угроза реализуется одним из двух способов: путем внутрисегментного или межсегментного навязывания. Возможность навязывания ложного маршрута обусловлена недостатками, присущими

алгоритмам маршрутизации (в частности из- за проблемы идентификации сетевых управляющих устройств), в результате чего можно попасть, например, на хост или в сеть злоумышленника, где можно войти в операционную среду технического средства в составе ИСПДн. Реализации угрозы основывается на несанкционированном использовании протоколов маршрутизации (RIP, OSPF, LSP) и управления сетью (ICMP, SNMP) для внесения изменений в маршрутно- адресные таблицы. При этом нарушителю необходимо послать от имени сетевого управляющего устройства (например, маршрутизатора) управляющее сообщение.

На границе сети используется сертифицированный межсетевой экран. ИСПДн осуществляет межсетевое взаимодействие с использованием СКЗИ.

Вероятность реализации угрозы – низкая вероятность.

5.2.5.5. Угрозы подмены доверенного объекта

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

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

Процесс реализации с установлением виртуального соединения состоит в присвоении прав доверенного субъекта взаимодействия, что позволяет нарушителю вести сеанс работы с объектом сети от имени доверенного субъекта. Реализация угрозы данного типа требует преодоления системы идентификации и аутентификации сообщений (например, атака rsh- службы UNIX- хоста).

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

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

На границе сети используется сертифицированный межсетевой экран. ИСПДн осуществляет межсетевое взаимодействие с использованием СКЗИ.

Вероятность реализации угрозы – низкая вероятность.

5.2.5.6. Внедрение ложного объекта сети

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

На границе сети используется сертифицированный межсетевой экран. ИСПДн осуществляет межсетевое взаимодействие с использованием СКЗИ.

Вероятность реализации угрозы – низкая вероятность.

5.2.5.7. Угрозы типа « Отказ в обслуживании»

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

Могут быть выделены несколько разновидностей таких угроз:

- скрытый отказ в обслуживании, вызванный привлечением части ресурсов ИСПДн на обработку пакетов, передаваемых злоумышленником со снижением пропускной способности каналов связи, производительности сетевых устройств, нарушением требований к времени обработки запросов. Примерами реализации угроз подобного рода могут служить: направленный шторм эхо- запросов по протоколу ICMP (Ping flooding), шторм запросов на установление TCP- соединений (SYN- flooding), шторм запросов к FTP- серверу;

- явный отказ в обслуживании, вызванный исчерпанием ресурсов ИСПДн при обработке пакетов, передаваемых злоумышленником (занятие всей полосы пропускания каналов связи, переполнение очередей запросов

на обслуживание), при котором легальные запросы не могут быть переданы через сеть из- за недоступности среды передачи, либо получают отказ в обслуживании ввиду переполнения очередей запросов, дискового пространства памяти и т.д. Примерами угроз данного типа могут служить шторм широковещательных ICMP- эхо- запросов (Smurf), направленный шторм (SYN- flooding), шторм сообщений почтовому серверу (Spam);

- явный отказ в обслуживании, вызванный нарушением логической связности между техническим средствами ИСПДн при передаче нарушителем управляющих сообщений от имени сетевых устройств, приводящих к изменению маршрутно- адресных данных (например, ICMP Redirect Host, DNS- flooding) или идентификационной и аутентификационной информации;

- явный отказ в обслуживании, вызванный передачей злоумышленником пакетов с нестандартными атрибутами (угрозы типа « Land», « TearDrop», « Bonk», « Nuke», « UDP- bomb») или имеющих длину, превышающую максимально допустимый размер (угроза типа « Ping Death»), что может привести к сбою сетевых устройств, участвующих в обработке запросов, при условии наличия ошибок в программах, реализующих протоколы сетевого обмена.

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

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

Вероятность реализации угрозы – низкая вероятность.

5.2.5.8. Угрозы удаленного запуска приложений

Угроза заключается в стремлении запустить на хосте ИСПДн различные предварительно внедренные вредоносные программы: программы- закладки, вирусы, « сетевые шпионы», основная цель которых - нарушение конфиденциальности, целостности, доступности информации и полный контроль за работой хоста. Кроме того, возможен несанкционированный запуск прикладных программ пользователей для

несанкционированного получения необходимых нарушителю данных, для запуска управляемых прикладной программой процессов и др.

Выделяют три подкласса данных угроз:

- распространение файлов, содержащих несанкционированный исполняемый код;

- удаленный запуск приложения путем переполнения буфера приложений- серверов;

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

Типовые угрозы первого из указанных подклассов основываются на активизации распространяемых файлов при случайном обращении к ним. Примерами таких файлов могут служить: файлы, содержащие исполняемый код в вид документы, содержащие исполняемый код в виде элементов ActiveX, Java- апплетов, интерпретируемых скриптов (например, тексты на JavaScript); файлы, содержащие исполняемые коды программ. Для распространения файлов могут использоваться службы электронной почты, передачи файлов, сетевой файловой системы.

При угрозах второго подкласса используются недостатки программ, реализующих сетевые сервисы (в частности, отсутствие контроля за переполнением буфера). Настройкой системных регистров иногда удается переключить процессор после прерывания, вызванного переполнением буфера, на исполнение кода, содержащегося за границей буфера. Примером реализации такой угрозы может служить внедрение широко известного « вируса Морриса».

При угрозах третьего подкласса нарушитель использует возможности удаленного управления системой, предоставляемые скрытыми компонентами (например, « троянскими» программами типа Back. Orifice, Net Bus), либо штатными средствами управления и администрирования компьютерных сетей (Landesk Management Suite, Managewise, Back Orifice и т. п.). В результате их использования удается добиться удаленного контроля над станцией в сети.

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

Вероятность реализации угрозы – низкая вероятность.

5.2.5.9. Угрозы внедрения по сети вредоносных программ

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

Вредоносными программами, обеспечивающими осуществление НСД, могут быть:

- программы подбора и вскрытия паролей;
- программы, реализующие угрозы;
- программы, демонстрирующие использование недекларированных возможностей программного и программно- аппаратного обеспечения ИСПДн;
- программы- генераторы компьютерных вирусов;
- программы, демонстрирующие уязвимости средств защиты информации и др.

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

Вероятность реализации угрозы – низкая вероятность.

6. Реализуемость угроз

По итогам оценки уровня защищенности (Y_1) и вероятности реализации угрозы (Y_2), рассчитывается коэффициент реализуемости угрозы (Y) и определяется возможность реализации угрозы. Коэффициент реализуемости угрозы Y будет определяться соотношением $Y = (Y_1 + Y_2)/20$.

Оценка реализуемости УБПДн представлена в таблице.

Таблица 4. Реализуемость УБПДн

Тип угроз безопасности ПДн	Коэффициент реализуемости угрозы (Y)	Возможность реализации
1. Угрозы от утечки по техническим каналам.		
1.1. Угрозы утечки акустической информации	0,25	низкая
1.2. Угрозы утечки видовой информации	0,25	низкая

1.3. Угрозы утечки информации по каналам ПЭМИН	0,25	низкая
2. Угрозы несанкционированного доступа к информации.		
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн		
2.1.1. Кража ПЭВМ	0,25	низкая
2.1.2. Кража носителей информации	0,25	низкая
2.1.3. Кража ключей и атрибутов доступа	0,06	средняя
2.1.4. Кражи, модификации, уничтожения информации	0,06	средняя
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	0,25	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	0,06	средняя
2.1.7. Несанкционированное отключение средств защиты	0,06	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).		
2.2.1. Действия вредоносных программ (вирусов)	0,35	средняя
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	0,25	низкая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	0,5	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.		
2.3.1. Утрата ключей и атрибутов доступа	0,06	средняя
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	0,75	высокая

2.3.3. Непреднамеренное отключение средств защиты	0,06	средняя
2.3.4. Выход из строя аппаратно- программных средств	0,5	средняя
2.3.5. Сбой системы электроснабжения	0,25	низкая
2.3.6. Стихийное бедствие	0,25	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей		
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	0,06	средняя
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	0,25	низкая
2.5. Угрозы несанкционированного доступа по каналам связи.		
2.5.1. Угроза « Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:		
2.5.1.1. Перехват за переделами с контролируемой зоны	0,35	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	0,25	низкая
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	0,25	низкая
2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	0,5	средняя
2.5.3. Угрозы выявления паролей по сети	0,06	средняя
2.5.4. Угрозы навязывание ложного маршрута сети	0,35	средняя
2.5.5. Угрозы подмены доверенного объекта в сети	0,35	средняя
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	0,35	средняя
2.5.7. Угрозы типа « Отказ в обслуживании»	0,35	средняя
2.5.8. Угрозы удаленного запуска приложений	0,35	средняя

2.5.9. Угрозы внедрения по сети вредоносных программ	0,35	средняя

7. ОЦЕНКА ОПАСНОСТИ УГРОЗ

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

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

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

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

Оценка опасности УБПДн представлена таблице 5.

Таблица 5. Опасность УБПДн

Тип угроз безопасности ПДн	**Опасность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	низкая
1.2. Угрозы утечки видовой информации	низкая
1.3. Угрозы утечки информации по каналам ПЭМИН	низкая
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	низкая
2.1.2. Кража носителей информации	низкая
2.1.3. Кража ключей и атрибутов доступа	низкая
2.1.4. Кражи, модификации, уничтожения информации	низкая
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	низкая
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая
2.1.7. Несанкционированное отключение средств защиты	низкая
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).	
2.2.1. Действия вредоносных программ (вирусов)	низкая
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	низкая
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	низкая
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.	
2.3.1. Утрата ключей и атрибутов доступа	низкая
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	низкая
2.3.3. Непреднамеренное отключение средств защиты	низкая
2.3.4. Выход из строя аппаратно- программных средств	низкая
2.3.5. Сбой системы электроснабжения	низкая
2.3.6. Стихийное бедствие	низкая
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенными к ее обработке	низкая
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	низкая
2.5. Угрозы несанкционированного доступа по каналам связи.	
2.5.1. Угроза « Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	низкая
2.5.1.1. Перехват за переделами с контролируемой зоны	низкая
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	низкая
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	низкая
2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	низкая
2.5.3. Угрозы выявления паролей по сети	низкая

2.5.4. Угрозы навязывание ложного маршрута сети	низкая
2.5.5. Угрозы подмены доверенного объекта в сети	низкая
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	низкая
2.5.7. Угрозы типа « Отказ в обслуживании»	низкая
2.5.8. Угрозы удаленного запуска приложений	низкая
2.5.9. Угрозы внедрения по сети вредоносных программ	низкая

8. ОПРЕДЕЛЕНИЕ АКТУАЛЬНОСТИ УГРОЗ В ИСПДН

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

Таблица 6. Правила определения актуальности УБПДн

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

Оценка актуальности угроз безопасности представлена в таблице 7.

Таблица 7. Актуальность УБПДн

Тип угроз безопасности ПДн	**Актуальность угрозы**
1. Угрозы от утечки по техническим каналам.	
1.1. Угрозы утечки акустической информации	неактуальная
1.2. Угрозы утечки видовой информации	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	неактуальная
2. Угрозы несанкционированного доступа к информации.	
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн	
2.1.1. Кража ПЭВМ	неактуальная
2.1.2. Кража носителей информации	неактуальная
2.1.3. Кража ключей и атрибутов доступа	неактуальная
2.1.4. Кражи, модификации, уничтожения информации	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	неактуальная
2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	неактуальная
2.1.7. Несанкционированное отключение средств защиты	неактуальная
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).	

2.2.1. Действия вредоносных программ (вирусов)	неактуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	неактуальная
2.2.3. Установка ПО не связанного с исполнением служебных обязанностей	неактуальная
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.	
2.3.1. Утрата ключей и атрибутов доступа	неактуальная
2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	актуальная
2.3.3. Непреднамеренное отключение средств защиты	неактуальная
2.3.4. Выход из строя аппаратно- программных средств	неактуальная
2.3.5. Сбой системы электроснабжения	неактуальная
2.3.6. Стихийное бедствие	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей	
2.4.1. Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	неактуальная
2.5. Угрозы несанкционированного доступа по каналам связи.	
2.5.1. Угроза « Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:	
2.5.1.1. Перехват за переделами с контролируемой зоны	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями	неактуальная
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	неактуальная
2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	неактуальная
2.5.3. Угрозы выявления паролей по сети	неактуальная
2.5.4. Угрозы навязывание ложного маршрута сети	неактуальная

2.5.5. Угрозы подмены доверенного объекта в сети	неактуальная
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн, так и во внешних сетях	неактуальная
2.5.7. Угрозы типа « Отказ в обслуживании»	неактуальная
2.5.8. Угрозы удаленного запуска приложений	неактуальная
2.5.9. Угрозы внедрения по сети вредоносных программ	неактуальная

Были выявлены следующие актуальные угрозы для обрабатываемых персональных данных:

1) Непреднамеренная модификация (уничтожение) информации сотрудниками

Для снижения вероятности реализации и опасности угроз безопасности ПДн рекомендуется осуществить следующие мероприятия:

1. Регулярно выполнять резервное копирование данных ИСПДн.

2. Проводить периодический контроль работоспособности средств защиты информации.

3. Использовать лицензионное программное обеспечение, позволяющее получать техническую поддержку и обновление системы защиты со стороны разработчика.

9. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ

В соответствии с п 4. настоящей Модели угроз, исходный уровень защищенности ПДн – средний (Y1=5).

Таблица 1. Угрозы безопасности

Наименование угрозы	**Вероятность реализации угрозы (Y2)**	**Возможность реализации угрозы (Y)**	**Опасность угрозы**	**Актуальность угрозы**
1. Угрозы от утечки по техническим каналам				
1.1. Угрозы утечки акустической информации	маловероятна	низкая	низкая	неактуальная
1.2. Угрозы утечки видовой информации	маловероятна	низкая	низкая	неактуальная
1.3. Угрозы утечки информации по каналам ПЭМИН	маловероятна	низкая	низкая	неактуальная
2. Угрозы несанкционированного доступа к информации				
2.1. Угрозы уничтожения, хищения аппаратных средств ИСПДн носителей информации путем физического доступа к элементам ИСПДн				
2.1.1. Кража ПЭВМ	маловероятна	низкая	низкая	неактуальная
2.1.2. Кража носителей информации	маловероятна	низкая	низкая	неактуальная
2.1.3. Кража ключей доступа	низкая вероятность	средняя	низкая	неактуальная
2.1.4. Кражи, модификации, уничтожения информации.	низкая вероятность	средняя	низкая	неактуальная
2.1.5. Вывод из строя узлов ПЭВМ, каналов связи	маловероятна	низкая	низкая	неактуальная

2.1.6. Несанкционированный доступ к информации при техническом обслуживании (ремонте, уничтожении) узлов ПЭВМ	низкая вероятность	средняя	низкая	неактуальная
2.1.7. Несанкционированное отключение средств защиты	низкая вероятность	средняя	низкая	неактуальная
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);				
2.2.1. Действия вредоносных программ (вирусов)	низкая вероятность	средняя	низкая	неактуальная
2.2.2. Недекларированные возможности системного ПО и ПО для обработки персональных данных	маловероятна	низкая	низкая	неактуальная
2.2.3. Установка ПО, не связанного с исполнением служебных обязанностей	средняя вероятность	средняя	низкая	неактуальная
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.				
2.3.1. Утрата ключей и атрибутов доступа	низкая вероятность	средняя	низкая	неактуальная

2.3.2. Непреднамеренная модификация (уничтожение) информации сотрудниками	низкая вероятность	средняя	низкая	неактуальная
2.3.3. Непреднамеренное отключение средств защиты	низкая вероятность	средняя	низкая	неактуальная
2.3.4. Выход из строя аппаратно-программных средств	средняя вероятность	средняя	низкая	неактуальная
2.3.5. Сбой системы электроснабжения	маловероятна	низкая	низкая	неактуальная
2.3.6. Стихийное бедствие	маловероятна	низкая	низкая	неактуальная
2.4. Угрозы преднамеренных действий внутренних нарушителей				
2.4.1. Доступ к информации, модификация, уничтожение лицами не допущенных к ее обработке	низкая вероятность	средняя	низкая	неактуальная
2.4.2. Разглашение информации, модификация, уничтожение сотрудниками, допущенными к ее обработке	маловероятна	низкая	низкая	неактуальная
2.5. Угрозы несанкционированного доступа по каналам связи				
2.5.1. Угроза « Анализ сетевого трафика» с перехватом передаваемой из ИСПДн и принимаемой из внешних сетей информации:				

2.5.1.1. Перехват за переделами с контролируемой зоны;	маловероятна	низкая	низкая	неактуальная
2.5.1.2. Перехват в пределах контролируемой зоны внешними нарушителями;	маловероятна	низкая	низкая	неактуальная
2.5.1.3. Перехват в пределах контролируемой зоны внутренними нарушителями.	маловероятна	низкая	низкая	неактуальная
2.5.2. Угрозы сканирования, направленные на выявление типа или типов используемых операционных систем, сетевых адресов рабочих станций ИСПДн, топологии сети, открытых портов и служб, открытых соединений и др.	маловероятна	низкая	низкая	неактуальная
2.5.3. Угрозы выявления паролей по сети.	низкая вероятность	средняя	низкая	неактуальная
2.5.4. Угрозы навязывание ложного маршрута сети.	маловероятна	низкая	низкая	неактуальная
2.5.5. Угрозы подмены доверенного объекта в сети.	маловероятна	низкая	низкая	неактуальная
2.5.6. Угрозы внедрения ложного объекта как в ИСПДн,	маловероятно	низкая	низкая	неактуальная

так и во внешних сетях.				
2.5.7. Угрозы типа « Отказ в обслуживании».	маловероятно	низкая	низкая	неактуальная
2.5.8. Угрозы удаленного запуска приложений.	маловероятно	низкая	низкая	неактуальная
2.5.9. Угрозы внедрения по сети вредоносных программ.	маловероятно	низкая	низкая	неактуальная

10. ПЕРЕЧЕНЬ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ БАНКА ДАННЫХ УГРОЗ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

На основе проведенного анализа угроз Банка данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю Российской Федерации с учетом структурно-функциональных характеристик ИСПДн, применяемых в ИСПДн информационных технологий, особенностей функционирования, анализа потенциала вероятного нарушителя для ИСПДн актуальны угрозы, приведенные в таблице 11.

Таблица 11. Перечень актуальных угроз безопасности персональных данных банка данных угроз безопасности информации.

№ п/п	Идентификатор угрозы	Наименование угрозы безопасности информации
1.	4	Угроза аппаратного сброса пароля BIOS
2.	6	Угроза внедрения кода или данных
3.	8	Угроза восстановления аутентификационной информации
4.	9	Угроза восстановления предыдущей уязвимой версии BIOS
5.	12	Угроза деструктивного изменения конфигурации/ среды окружения программ
6.	13	Угроза деструктивного использования декларированного функционала BIOS
7.	14	Угроза длительного удержания вычислительных ресурсов пользователями
8.	15	Угроза доступа к защищаемым файлам с использованием обходного пути
9.	18	Угроза загрузки нештатной операционной системы
10.	19	Угроза заражения DNS- кеша
11.	22	Угроза избыточного выделения оперативной памяти
13.	23	Угроза изменения компонентов системы
13.	27	Угроза искажения вводимой и выводимой на периферийные устройства информации
14.	28	Угроза использования альтернативных путей доступа к ресурсам

15.	30	Угроза использования информации идентификации/ аутентификации, заданной по умолчанию
16.	31	Угроза использования механизмов авторизации для повышения привилегий
17.	34	Угроза использования слабостей протоколов сетевого/ локального обмена данными
18.	45	Угроза нарушения изоляции среды исполнения BIOS
19.	46	Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
20.	49	Угроза нарушения целостности данных кеша
21.	51	Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
22.	52	Угроза невозможности миграции образов виртуальных машин из- за несовместимости аппаратного и программного обеспечения
23.	53	Угроза невозможности управления правами пользователей BIOS
24.	58	Угроза неконтролируемого роста числа виртуальных машин
25.	59	Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
26.	67	Угроза неправомерного ознакомления с защищаемой информацией
27.	69	Угроза неправомерных действий в каналах связи
28.	71	Угроза несанкционированного восстановления удалённой защищаемой информации
29.	72	Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
30.	74	Угроза несанкционированного доступа к аутентификационной информации
31.	75	Угроза несанкционированного доступа к виртуальным каналам передачи
32.	78	Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
33.	79	Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
34.	84	Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
35.	86	Угроза несанкционированного изменения аутентификационной информации
36.	87	Угроза несанкционированного использования привилегированных функций BIOS

37.	88	Угроза несанкционированного копирования защищаемой информации
38.	89	Угроза несанкционированного редактирования реестра
39.	90	Угроза несанкционированного создания учётной записи пользователя
40.	91	Угроза несанкционированного удаления защищаемой информации
41.	93	Угроза несанкционированного управления буфером
42.	98	Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
43.	99	Угроза обнаружения хостов
44.	100	Угроза обхода некорректно настроенных механизмов аутентификации
45.	103	Угроза определения типов объектов защиты
46.	104	Угроза определения топологии вычислительной сети
47.	108	Угроза ошибки обновления гипервизора
48.	113	Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
49.	115	Угроза перехвата вводимой и выводимой на периферийные устройства информации
50.	116	Угроза перехвата данных, передаваемых по вычислительной сети
51.	121	Угроза повреждения системного реестра
52.	123	Угроза подбора пароля BIOS
53.	124	Угроза подделки записей журнала регистрации событий
54.	128	Угроза подмены доверенного пользователя
55.	129	Угроза подмены резервной копии программного обеспечения BIOS
56.	130	Угроза подмены содержимого сетевых ресурсов
57.	140	Угроза приведения системы в состояние «отказ в обслуживании»
58.	144	Угроза программного сброса пароля BIOS
59.	145	Угроза пропуска проверки целостности программного обеспечения
60.	152	Угроза удаления аутентификационной информации
61.	153	Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
62.	155	Угроза утраты вычислительных ресурсов
63.	156	Угроза утраты носителей информации
64.	157	Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
65.	158	Угроза форматирования носителей информации
66.	160	Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации

67.	162	Угроза эксплуатации цифровой подписи программного кода
68.	167	Угроза заражения компьютера при посещении неблагонадёжных сайтов
69.	168	Угроза «кражи» учётной записи доступа к сетевым сервисам
70.	170	Угроза неправомерного шифрования информации
71.	171	Угроза скрытного включения вычислительного устройства в состав бот-сети
72.	172	Угроза распространения «почтовых червей»
73.	177	Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью
74.	178	Угроза несанкционированного использования системных и сетевых утилит
75.	179	Угроза несанкционированной модификации защищаемой информации
76.	180	Угроза отказа подсистемы обеспечения температурного режима
77.	182	Угроза физического устаревания аппаратных компонентов
78.	185	Угроза несанкционированного изменения параметров настройки средств защиты информации
79.	186	Угроза внедрения вредоносного кода через рекламу, сервисы и контент
80.	191	Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
81.	192	Угроза использования уязвимых версий программного обеспечения
82.	205	Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты
83.	208	Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
84.	209	Угроза несанкционированного доступа к защищаемой памяти ядра процессора
85.	211	Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем

11. ИСПОЛЬЗОВАНИЕ СКЗИ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДн

11.1. Использование СКЗИ для обеспечения безопасности ПДн

Передача персональных данных в (из, внутри) ИСПДн по каналам связи, не защищенным от перехвата нарушителем передаваемой по ним информации или от несанкционированных воздействий на эту информацию (например, при передаче персональных данных по информационно-телекоммуникационным сетям общего пользования) осуществляется с использованием СКЗИ.

11.2. Объекты защиты ИСПДн

К объектам защиты ИСПДн, относятся:

- персональные данные;
- СКЗИ;
- среда функционирования СКЗИ (СФ);
- информация, относящаяся к криптографической защите персональных данных, включая ключевую, парольную и аутентифицирующую информацию СКЗИ;
- документы, дела, журналы, картотеки, издания, технические документы, видео-, кино- и фотоматериалы, рабочие материалы и т.п., в которых отражена защищаемая информация, относящаяся к информационным системам персональных данных и их криптографической защите, включая документацию на СКЗИ и на технические и программные компоненты СФ;
- носители защищаемой информации, используемые в информационной системе в процессе криптографической защиты персональных данных, носители ключевой, парольной и аутентифицирующей информации СКЗИ и порядок доступа к ним;
- используемые информационной системой каналы (линии) связи, включая кабельные системы;
- помещения, в которых находятся ресурсы информационной системы, имеющие отношение к криптографической защите персональных данных.

11.3. Актуальность возможностей нарушителей и направления атак

Реализация угроз безопасности персональных данных, обрабатываемых в информационных системах персональных данных, определяется возможностями источников атак. Таким образом, актуальность использования возможностей источников атак определяет наличие соответствующих актуальных угроз.

На основании исходных данных об объектах защиты, источников атак, оценке возможного вреда субъекту персональных данных определены обобщенные возможности источников атак. Обобщенные возможности источников атак приведены в таблице 9.

Таблица 9. Обобщенные возможности источников атак

№ п/п	Обобщенные возможности источников атак	Да/нет
1.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак только за пределами контролируемой зоны	да
2.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны, но без физического доступа к аппаратным средствам (далее - АС), на которых реализованы СКЗИ и среда их функционирования	нет
3.	Возможность самостоятельно осуществлять создание способов атак, подготовку и проведение атак в пределах контролируемой зоны с физическим доступом к АС, на которых реализованы СКЗИ и среда их функционирования	нет
4.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области анализа сигналов линейной передачи и сигналов побочного электромагнитного излучения и наводок СКЗИ)	нет
5.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения);	нет
6.	Возможность привлекать специалистов, имеющих опыт разработки и анализа СКЗИ (включая специалистов в области использования для реализации атак недокументированных возможностей аппаратного и программного компонентов среды функционирования СКЗИ).	нет

Таблица 10. Актуальность возможностей нарушителей и направления атак

№ п/п	Уточненные возможности нарушителей и направления атак (соответствующие актуальные угрозы)	Актуальность использования (применения) для построения и реализации атак	Обоснование отсутствия
1.1.	проведение атаки при нахождении в пределах контролируемой зоны.	неактуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с внутренними локальными актами; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены СКЗИ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; сотрудники, являющиеся пользователями ИСПДн, но не являющиеся пользователями СКЗИ, проинформированы о правилах работы в ИСПДн и ответственности за несоблюдение правил обеспечения безопасности информации; пользователи СКЗИ проинформированы о правилах работы в ИСПДн, правилах работы с СКЗИ и ответственности за несоблюдение правил обеспечения безопасности информации; помещения, в которых располагаются СКЗИ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытия только для санкционированного прохода; утверждены правила доступа в помещения, где располагаются СКЗИ,

			в рабочее и нерабочее время, а также в нештатных ситуациях; утвержден перечень лиц, имеющих право доступа в помещения, где располагаются СКЗИ; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей с ПДн; осуществляется контроль целостности средств защиты; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
1.2.	проведение атак на этапе эксплуатации СКЗИ на следующие объекты: - документацию на СКЗИ и компоненты СФ; - помещения, в которых находится совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (далее - СВТ), на которых реализованы СКЗИ и СФ.	неактуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с внутренними локальными актами; документация на СКЗИ хранится у ответственного за СКЗИ в металлическом сейфе; помещение, в которых располагаются документация на СКЗИ, СКЗИ и компоненты СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; утвержден перечень лиц, имеющих право доступа в помещения.
1.3.	получение в рамках предоставленных полномочий, а также в результате наблюдений следующей информации:	неактуально	проводятся работы по подбору персонала; доступ в контролируемую зону, где располагается СКЗИ, обеспечивается в соответствии с внутренними локальными актами;

	- сведений о физических мерах защиты объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по обеспечению контролируемой зоны объектов, в которых размещены ресурсы информационной системы; - сведений о мерах по разграничению доступа в помещения, в которых находятся СВТ, на которых реализованы СКЗИ и СФ.		сведения о физических мерах защиты объектов, в которых размещены ИСПДн, доступны ограниченному кругу сотрудников; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации.
1.4.	использование штатных средств ИСПДн, ограниченное мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	неактуально	проводятся работы по подбору персоналов; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; сотрудники проинформированы об ответственности за несоблюдение правил обеспечения безопасности информации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; в ИСПДн используются: сертифицированные средства защиты информации от несанкционированного доступа; сертифицированные средства антивирусной защиты.

2.1.	физический доступ к СВТ, на которых реализованы СКЗИ и СФ.	неактуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с внутренними локальными актами; помещения, в которых располагаются СВТ, на которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода.
2.2.	возможность воздействовать на аппаратные компоненты СКЗИ и СФ, ограниченная мерами, реализованными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.	неактуально	проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с внутренними локальными актами; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации.
3.1.	создание способов, подготовка и проведение атак с привлечением специалистов в области анализа сигналов, сопровождающих	неактуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность

	функционирование СКЗИ и СФ, и в области использования для реализации атак недокументированных (недекларированных) возможностей прикладного ПО.		подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с внутренними локальными актами; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
3.2.	проведение лабораторных исследований СКЗИ, используемых вне контролируемой зоны, ограниченное мерами, реализован-	неактуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.

	ными в информационной системе, в которой используется СКЗИ, и направленными на предотвращение и пресечение несанкционированных действий.		
3.3.	проведение работ по созданию способов и средств атак в научно-исследовательских центрах, специализирующихся в области разработки и анализа СКЗИ и СФ, в том числе с использованием исходных текстов входящего в СФ прикладного ПО, непосредственно использующего вызовы программных функций СКЗИ.	неактуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности.
4.1.	создание способов, подготовка и проведение атак с привлечением специалистов в области использования для реализации атак недокументированных (недекларированных) возможностей системного ПО.	неактуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности; высокая стоимость и сложность подготовки реализации возможности; проводятся работы по подбору персонала; доступ в контролируемую зону и помещения, где располагается СВТ, на которых реализованы СКЗИ и СФ, обеспечивается в соответствии с внутренними локальными актами; помещения, в которых располагаются СКЗИ и СФ, оснащены входными дверьми с замками, обеспечивается постоянное закрытие дверей

			помещений на замок и их открытие только для санкционированного прохода; представители технических, обслуживающих и других вспомогательных служб при работе в помещениях (стойках), где расположены компоненты СКЗИ и СФ, и сотрудники, не являющиеся пользователями СКЗИ, находятся в этих помещениях только в присутствии сотрудников по эксплуатации; осуществляется разграничение и контроль доступа пользователей к защищаемым ресурсам; осуществляется регистрация и учет действий пользователей; на АРМ и серверах, на которых установлены СКЗИ: используются сертифицированные средства защиты информации от несанкционированного доступа; используются сертифицированные средства антивирусной защиты.
4.2.	возможность располагать сведениями, содержащимися в конструкторской документации на аппаратные и программные компоненты СФ.	неактуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.
4.3.	возможность воздействовать на любые компоненты СКЗИ и СФ.	неактуально	не осуществляется обработка сведений, составляющих государственную тайну, а также иных сведений, которые могут представлять интерес для реализации возможности.

12. ЗАКЛЮЧЕНИЕ

Ввиду исключительной роли в ИСПДн лиц категорий I и II в число этих лиц должны включаться только доверенные лица, к которым применен комплекс организационных мер по их подбору, принятию на работу, назначению на должность и контролю выполнения функциональных обязанностей.

Лица категорий III-VII относятся к вероятным нарушителям.

Среди лиц категорий III-VII наиболее опасными вероятными нарушителями являются лица категории III и лица категорий V-VI (уполномоченный персонал разработчиков ИСПДн, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИСПДн, бывшие сотрудники).

ИСПДн имеет внешние источники атак не имеющие возможности доступа к объектам защиты. Однако способных осуществлять создание способов атак, подготовку и проведение атак за пределами контролируемой зоны.

Передача персональных данных ИСПДн по информационно-телекоммуникационным сетям общего пользования осуществляется с использованием СКЗИ.

При использовании СКЗИ для обеспечения безопасности персональных данных, необходимо учитывать следующее:

- криптографическая защита персональных данных может быть обеспечена при условии отсутствия возможности несанкционированного доступа нарушителя к ключевой информации СКЗИ;

- СКЗИ штатно функционируют совместно с техническими и программными средствами, которые способны повлиять на выполнение предъявляемых к СКЗИ требований и которые образуют среду функционирования СКЗИ;

- СКЗИ не предназначены для защиты информации от действий, выполняемых в рамках предоставленных субъекту действий полномочий (например, СКЗИ не предназначены для защиты персональных данных от раскрытия лицами, которым предоставлено право на доступ к этой информации);

- СКЗИ обеспечивают защиту информации при условии соблюдения требований эксплуатационно-технической документации на СКЗИ и требований, действующих нормативных правовых документов в области реализации и эксплуатации СКЗИ;

- для обеспечения безопасности персональных данных при их обработке в ИСПДн должны использоваться СКЗИ, прошедшие в установленном порядке процедуру оценки соответствия. Перечень СКЗИ, сертифицированных ФСБ России, опубликован на официальном сайте Центра по лицензированию, сертификации и защите государственной тайны ФСБ России (clsz.fsb.ru).

- СКЗИ являются как средством защиты персональных данных, так и объектом защиты.

Представленная модель угроз для ИСПДн должна использоваться при формировании обоснованных требований информационной безопасности и проектировании ИСПДн.

Для предотвращения возможности реализации актуальных угроз безопасности необходимо:

- регулярно выполнять резервное копирование данных ИСПДн;

- использовать лицензионное программное обеспечение, позволяющее получать техническую поддержку и обновление системы защиты со стороны разработчика.

- проводить периодический контроль работоспособности средств защиты информации;

- средства защиты информации от несанкционированного доступа эксплуатировать в соответствии с инструкцией и согласно Разрешительной системы доступа.

- организовать эксплуатацию СКЗИ в соответствии с инструкцией, правилами пользования и другими действующими нормативными документами.

«_____» _____20___ г.

Председатель комиссии:

Члены комиссии:

ПРИЛОЖЕНИЕ В

СПРАВКА

о результатах внедрения решений,
разработанных в выпускной квалификационной работе студентом
Амурского государственного университета

Бурдуковским Данилом Витальевичем
(ф.и.о. полностью)

В работе над ВКР по теме «Разработка и внедрение информационной системы с локальным чатом для сотрудников» студент принял непосредственное участие в разработке информационной системы с локальным чатом для сотрудников.

Полученные им результаты нашли отражение в методических разработках, в докладных и аналитических записках ГАУ ДПО «АмИРО» Региональный модельный центр.

В настоящее время методические разработки, включающие результаты данной выпускной квалификационной работы, включены в инструктивные материалы.

Руководитель
Борзунова Ю.В _____

М.П.