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 информационной системы «Контроль исполнения поручений»

Исполнитель
студент группы 755-об _____ Т.Н. Бакланова
(подпись, дата)

Руководитель
доцент, канд.техн.наук _____ С.Г. Самохвалова
(подпись, дата)

Консультант
по безопасности
и экологичности
доцент, канд.техн.наук _____ А.Б. Булгаков
(подпись, дата)

Нормоконтроль
доцент, канд.техн.наук _____ О.В. Жилиндина
(подпись, дата)

Благовещенск 2021

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

УТВЕРЖДАЮ
Зав.кафедрой
_____ А.В. Бушманов

«_____»_____2021 г.

З А Д А Н И Е

К бакалаврской работе студента Баклановой Тамары Николаевны

1 Тема выпускной квалификационной работы: Разработка информационной системы «Контроль исполнения поручений».

(утверждена приказом от 24.05.2021 № 1008)

2 Срок сдачи студентом законченной работы: 24.06.2021

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

4 Содержание бакалаврской работы (перечень подлежащих разработке вопросов): анализ объекта исследования, анализ организационной структуры, анализ документооборота, проектирование базы данных, разработка информационной системы, техническое задание, анализ угроз информационной безопасности объекта исследования, анализ безопасности и экологичности объекта исследования.

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

6 Дата выдачи задания: 20.02.2021

Руководитель бакалаврской работы: доцент, канд. техн. наук. С.Г. Самохвалова

Задание принял к исполнению: 20.02.2021_____

(подпись студента)

РЕФЕРАТ

Бакалаврская работа содержит 102 с., 38 рисунка, 18 таблиц, 21 источник.

РАЗРАБОТКА ИНФОРМАЦИОННОЙ СИСТЕМЫ, ПРОЕКТИРОВАНИЕ БАЗЫ ДАННЫХ, ОРГАНИЗАЦИОННАЯ СТРУКТУРА, ДОКУМЕНТООБОРОТ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Субъектом данной работы является Центр информационных технологий, связи и защиты информации УМВД России по Амурской области.

Целью работы является разработка информационной системы «Контроль исполнения поручений».

Для достижения цели работы были выполнены следующие задачи: исследована организационная структура и деятельность сотрудников Центра информационных технологий, связи и защиты информации, сформировано техническое задание на разработку информационной системы «Контроль исполнения поручений». Также разработана структура базы данных и информационная система. Выполнена программная реализация информационной системы и ее тестирование. Исследован Центр информационных технологий, связи и защиты информации УМВД России по Амурской области на предмет угроз информационной безопасности, на предмет соответствия безопасности и экологичности.

В результате работы разработана информационная система «Контроль исполнения поручений», позволяющая повысить качество выполнения задач, возложенных на Центр информационных технологий, связи и защиты информации УМВД России по Амурской области.

СОДЕРЖАНИЕ

Введение 8
1 Анализ деятельности предприятия 10
1.1 Организационная структура 10
1.2 Основные задачи центра 13
1.3 Функциональная модель 14
1.4 Документооборот 16
1.5 Внешний документооборот 16
1.6 Внутренний документооборот 17
1.7 Объект и предмет защиты 18
1.8 Угрозы защищаемой информации 20
2 Описание комплексной системы защиты информации 28
2.1 Этапы построения комплексной системы защиты информации для УМВД России по Амурской области 28
2.2 Комплексная система защиты 29
2.3 Назначение и цели разработки информационной системы 30
2.4 Инфологическое проектирование 33
2.5 Логическое проектирование 41
2.6 Физическое проектирование 46
2.7 Руководство пользователя 48
3 ИСОД как современный этап развития ЕИТКС 55
3.1 Задачи создания СУДИС 59
3.2 Трудности внедрения 62
4 Безопасность и экологичность 64
4.1 Безопасность жизнедеятельности программиста 64
4.1.1 Требования к ПЭВМ 64
4.1.2 Требования к помещениям 64

4.1.3 Организация рабочего места 65
4.1.4 Требования к эргономичности программного продукта 67
4.2 Экологичность 68
4.2.1 Утилизация бумажных отходов 68
4.2.2 Утилизация компьютерной техники и оргтехники 69
4.2.3 Утилизация ламп 69
4.3 Чрезвычайные ситуации 70
4.3.1 Требования электробезопасности 70
4.3.2 Требования по обеспечению пожарной безопасности 71
4.4 Комплексы физических упражнений для сохранения и укрепления индивидуального здоровья и обеспечения полноценной профессиональной деятельности 72
4.4.1 Упражнения для глаз 72
4.4.2 Упражнения для головы и шеи 73
4.4.3 Упражнения для рук 73
4.4.4 Упражнения для туловища 74
Заключение 75
Библиографический список 76
Приложение А Техническое задание 79
Приложение Б Программный интерфейс 101

НОРМАТИВНЫЕ ССЫЛКИ

В настоящей бакалаврской работе использованы ссылки на следующие стандарты и нормативные документы:

ГОСТ 2.104-68 ЕСКД Основные надписи

ГОСТ 2.105-95 ЕСКД Общие требования к текстовым документам

ГОСТ 2.111-68 ЕСКД Нормоконтроль

ГОСТ 19.201-78 ЕСПД Техническое задание. Требования к содержанию и оформлению

ГОСТ 34.601-90 КСАС Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания

ГОСТ 34.602-89 КСАС Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы управления

ГОСТ 19.502-78 Описание применения. Требования к содержанию и оформлению

ГОСТ 19.505-79 Руководство оператора. Требования к содержанию и оформлению

ГОСТ 7.1-2003 Библиографическое описание документа. Общие требования и правила составления

ОПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АРМ – автоматизированные рабочие места;

АС – автоматизированные системы;

ЕАИС ЭКП – Сервис экспертно-криминалистической деятельности;

ИБД – Интегрированный банк данных;

ИСОД – единой системы информационно-аналитического обеспечения деятельности;

КСЗИ – комплексная система защиты информации;

МОСТ – Сервис статистической отчетности МВД РФ;

Ретроспектива – Единый банк данных архивной информации;

СОДИ – Сервис НЦБ Интерпола;

СОДЧ – Сервис обеспечения деятельности дежурных частей;

СОМТО – Сервис обеспечения деятельности подразделений материально-технического обеспечения МВД РФ;

СООП – Сервис обеспечения охраны общественного порядка;

СОПД ГУСБ – Сервис ГУ Собственной безопасности МВД;

СОПС – Сервис оформления проезда сотрудников;

СОЭБ – Сервис обеспечения экономической безопасности;

СПГУ – Сервис предоставления государственных услуг;

СУОГЗ – Сервис обеспечения государственной защиты лиц;

СЦУО – Система централизованного учета оружия;

УМВД РФ–Управление Министерства внутренних дел Российской Федерации;

ФИС ГИБДД-М – Федеральная информационная система ГИБДД МВД РФ;

ЦИАДИС-МВД – Банк отпечатков пальцев;

ЦИТСиЗИ – Центра информационных технологий, связи и защиты информации;

ЭВМ – Электронно-вычислительная машина.

ВВЕДЕНИЕ

Становление человечества в XXI веке характеризуется бурным внедрением информационных технологий во все сферы жизни и общества. Информация всё в большей степени воспринимается как стратегический ресурс государства, производительная сила и дорогой товар. Этот факт вызывает стремления государств, организаций и отдельных граждан получать преимущества за счет использования информации, недоступной конкурентам и за счет причинения вреда информационным ресурсам оппонента и защиты своих информационных ресурсов.

Информационные ресурсы становятся одними из главных источников экономической и иной эффективности организации. В настоящее время, можно наблюдать тенденцию, когда все сферы жизнедеятельности организации зависят от информационного обеспечения, в процессе которого они создают и потребляют информацию. В современных условиях развития основными угрозами безопасности организации являются угрозы в сфере информационного обеспечения. Следствием успешного проведения информационных воздействий становится компрометация или искажение конфиденциальной информации, навязывание ложной информации, нарушение установленного регламента сбора, обработки и передачи информации, отказы и сбои в работе технических систем, вызванные преднамеренными и непреднамеренными действиями, как со стороны конкурентов, так и со стороны преступных сообществ, организаций и групп.

Одной из ключевых задач в области безопасности предприятия следует считать создание комплексной системы защиты информации (далее КСЗИ). Ежегодно технические возможности злоумышленников совершенствуются. В связи с этим, информационные системы безопасности должны быть подготовлены к тому, чтобы дать отпор этим угрозам. Следовательно, необходимо стремиться построить такую систему безопасности, которая бы соответствовала

требованиям, предъявляемым к современным программам, и могла бы быть модернизирована, с целью сохранения надежности и актуальности.

Субъектом исследования является Центр информационных технологий, связи и защиты информации УМВД России по Амурской области.

Объектом исследования является информационная система «Контроль исполнения поручений» для ЦИТСиЗИ УМВД России по Амурской области.

Система защиты информации базируется на таких составляющих как, организационная, правовая, инженерно-техническая защита.

Целью бакалаврской работы является разработка информационной системы «Контроль исполнения поручений» для подразделения УМВД России по Амурской области – Центра информационных технологий, связи и защиты информации.

В рамках данной цели необходимо решить следующие задачи:

— проанализировать предметную область Центра;
— проанализировать внутренние и внешние процессы ЦИТС и ЗИ;
— изучить систему информационной безопасности ЦИТС и ЗИ;
— модернизировать существующую защиту ЦИТС и ЗИ;
— проектирование информационной системы;
— проанализировать безопасность и экологичность ЦИТС и ЗИ.

1 АНАЛИЗ ДЕЯТЕЛЬНОСТИ ПРЕДПРИЯТИЯ

Общая характеристика:

Объектом исследования, является одно из подразделений тыла УМВД России по Амурской области – Центр информационных технологий, связи и защиты информации. Центр выполняет задачи по защите информации в подразделениях УМВД России по Амурской области.

Основными направлениями деятельности Центра являются:

1 Обеспечение функционирования систем связи и передачи данных УМВД России по Амурской области.

2 Создание специализированных автоматизированных информационных систем органов полиции.

3 Использование радиочастотного спектра, применение радиоэлектронных средств и их электромагнитной совместимости.

4 Обеспечение функционирования действующей ведомственной системы связи в интересах подразделений полиции.

5 Определение приоритетных направлений по созданию и развитию ведомственной сети связи и их реализация в системе МВД.

1.1 Организационная структура

В Структуру УМВД России по Амурской области входят:

1 Следственное управление

2 Управление уголовного розыска

3 Управление по контролю за оборотом наркотиков

4 Управление экономической безопасности и противодействия коррупции

5 Управление по вопросам миграции

6 Управление по работе с личным составом

7 Управление государственной инспекции безопасности дорожного движения

8 Центр по противодействию экстремизму

9 Центр финансового обеспечения

10 Центр информационных технологий, связи и защиты информации

11 Центр кинологической службы

12 Центр профессиональной подготовки

13 Информационный центр

14 Экспертно-криминалистический центр

15 Дежурная часть

16 Оперативно-розыскная часть (по обеспечению безопасности лиц, подлежащих государственной защите)

17 Оперативно-розыскная часть собственной безопасности

18 Отдел оперативно-розыскной информации

19 Отдел организации дознания

20 Отдел организации деятельности участковых уполномоченных полиции и подразделений по делам несовершеннолетних

21 Отдел организации охраны общественного порядка на улицах и при проведении массовых мероприятий

22 Отдел организации охраны и конвоирования спец. учреждений полиции

23 Отдел организации применения административного законодательства

24 Отдел делопроизводства и режима

25 Отдел информации и общественных связей

26 Правовой отдел

27 Тыл

28 Штаб

29 ФКУ «Центр хозяйственного и сервисного обеспечения Управления Министерства внутренних дел Российской Федерации по Амурской области»

30 ФКУЗ «Медико-санитарная часть Министерства внутренних дел Российской Федерации по Амурской области»

31 Территориальные органы

На рисунке 1 представлена организационно-штатная структура Центра информационных технологий, связи и защиты информации УМВД России по Амурской области.

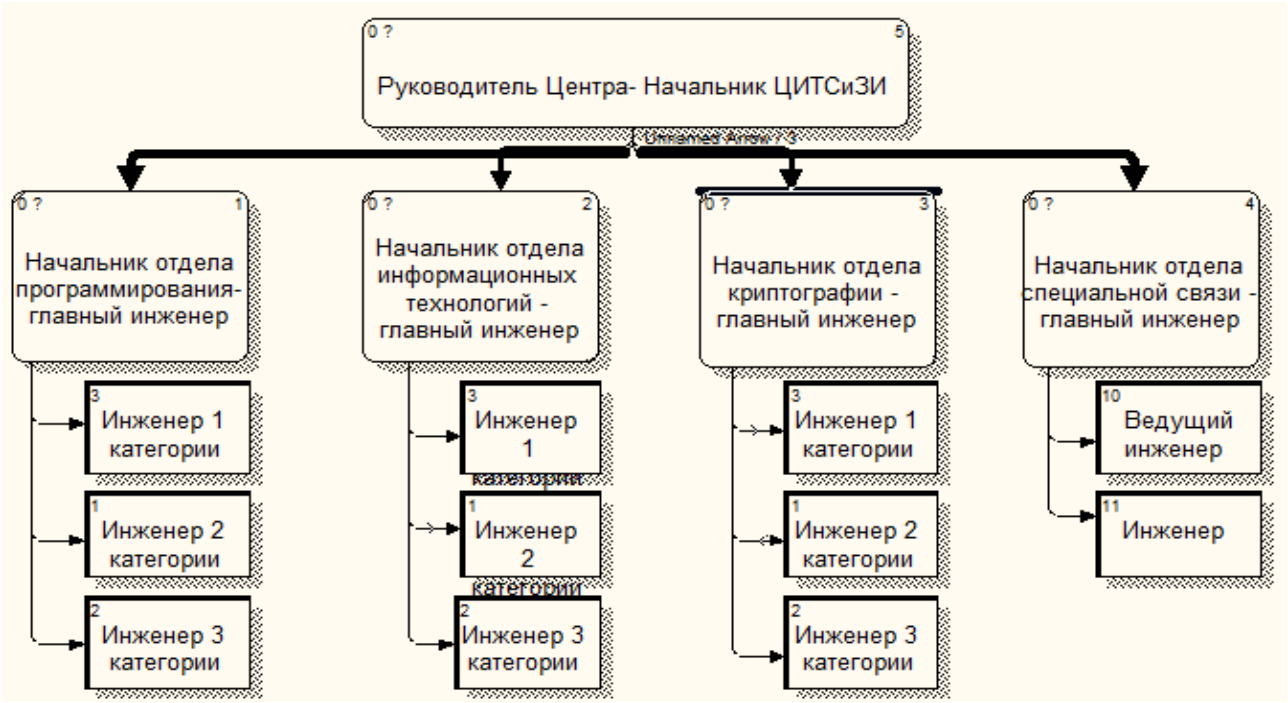

Рисунок 1 – Организационно-штатная структура Центра ИТСиЗИ

Функции отделов:

Отдел криптографии отвечает за разработку и использование электронных подписей, реализацию государственных и ведомственных программ в области информатизации, радиоэлектронную борьбу, формирования и ведения информационных ресурсов.

Отдел программирования отвечает за выявление нарушений правил эксплуатации ЭВМ, выявление незаконного проникновения в компьютерную сеть, вредоносных программ, системы ЭВМ или их сети, разработка электронных подписей для сотрудников, реализация государственных и ведомственных про-

грамм в области информатизации.

Отдел информационных технологий отвечает за бесперебойное функционирование оборудования и ПО в подразделениях, координацию работы по совершенствованию систем связи, автоматизирования информационных систем, техническую защиту информации, формирование и ведение информационных ресурсов.

1.2 Основные задачи Центра

Центр информационных технологий, связи и защиты информации в процессе своей деятельности выполняет следующие задачи:

1 использование современных информационных технологий в автоматизации технологических и производственных процессов;

2 использование информационно-вычислительной техники, средств передачи данных, программного обеспечения для реализации функций управления технологическими процессами и производственно-хозяйственной деятельностью Центра, и его подразделений;

3 содействие в использовании программно-аппаратных средств с целью обеспечения бесперебойной работы АРМ сотрудников Управления и его подразделений;

4 внедрение и проведение опытной эксплуатации ведомственных информационных систем, разработанных сотрудниками МВД России, с последующим их вводом в служебную эксплуатацию в аппарате управления и подразделениях;

5 совершенствование программного обеспечения эксплуатируемых задач, постановка новых задач, разработка их алгоритмов и программирование.

Общие функции Центра:

1 Планирование в области связи и автоматизации на объектах информатизации.

2 Обеспечение управления силами органов внутренних дел при повседневном несении службы.

3 Проведение мероприятий по проектированию, реконструкции и строительству сооружений связи.

4 Повышение профессионального мастерства сотрудников и работников подразделений связи органов внутренних дел области.

5 Списание и утилизация технических средств, в том числе лома и отходов, содержащих драгоценные металлы.

6 Обеспечение электромагнитной совместимости радиоэлектронных средств.

7 Проведение мероприятий по частотно-территориальному планированию.

8 Проведение опытной эксплуатации средств связи, систем передачи данных, готовит заключения по результатам.

1.3 Функциональная модель

Функциональная структура управления – это структура, сформированная в соответствии с основными направлениями деятельности организации, где подразделения объединяются в блоки.

Функция – самая существенная характеристика любой системы, отражает её предназначение, то, для чего она нужна. Подобные модели оперируют, прежде всего, с функциональными параметрами. Графическим представлением этих моделей служат блок-схемы. Они отображают порядок действий, направленных на достижение заданных целей. Функциональной моделью является абстрактная модель.

На функциональной модели можно увидеть информацию о взаимодействии организации с внешней средой, взаимодействии отделов внутри организации, о потоках информации, как вне организации, так и внутри.

На функциональной модели ЦИТСиЗИ, как и на любой другой, существуют: управляющая информация, механизмы, входы и выходы.

Управляющей информацией является Закон РФ от 21 июля 1993 г. № 5485-I «О государственной тайне».

На вход в систему идет информация из открытых источников, других региональных управлений МВД России программно-аппаратные средства, поступающие от поставщиков. На выход идёт ведомственные приказы, приказания и распоряжения руководителей подразделений МВД России, программно-аппаратные средства, прошедшие специальную проверку в подразделениях департамента ЦИТСиЗИ МВД России.

При поступлении информации из открытых источников, в подразделениях ЦИТСиЗИ проходит проверку на предмет соответствия действительности, а также законодательству РФ. На этапе обработки информации происходит выбор основных аспектов, с целью их дальнейшего применения при разработке ведомственных нормативно-правовых актов. Программно-аппаратные средства также подвергаются специальной проверке, в ходе которой устанавливается техническая защищенность аппаратуры, от возможных преступных посягательств. На основе данных построим функциональную модели и декомпозицию этой функциональной модели, изображенные на рисунке 2.

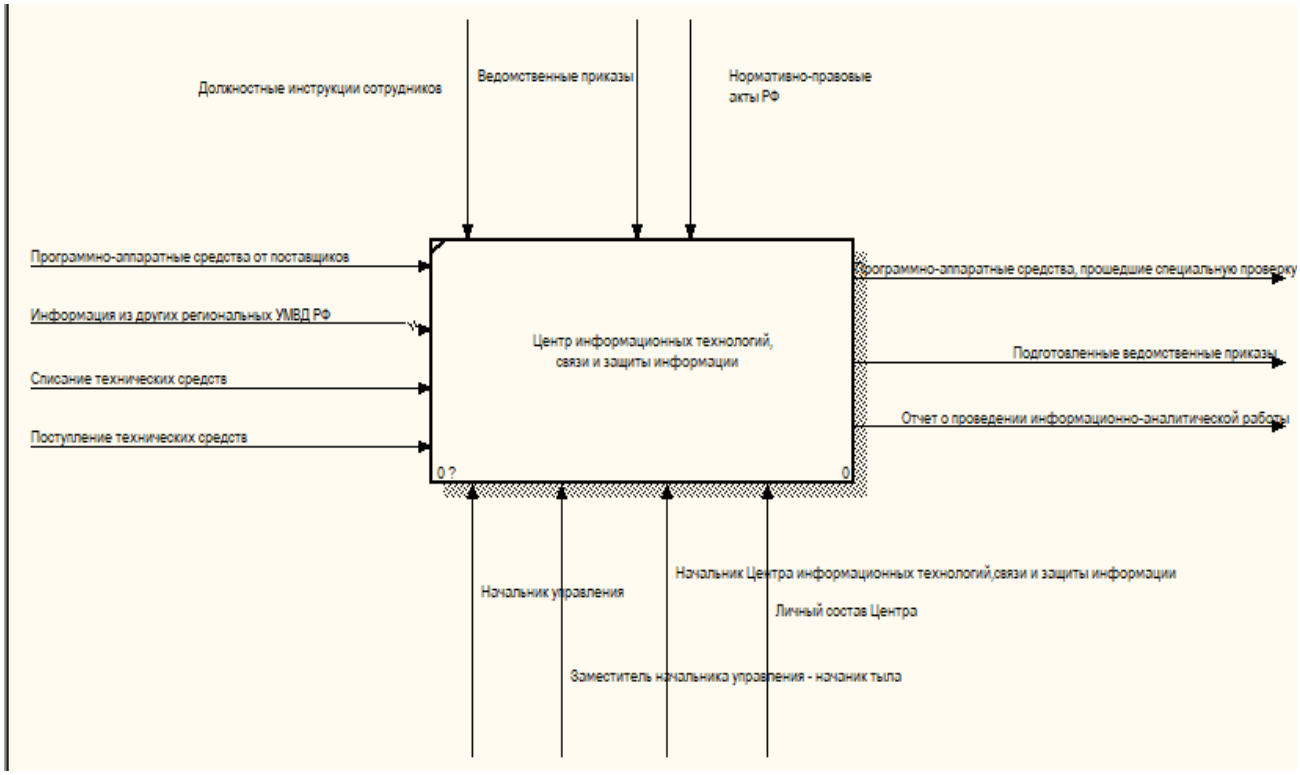

Рисунок 2 – Функциональная модель ЦИТСиЗИ

1.4 Документооборот

Электронный документооборот между пользователями системы, имеет большое значение для безбумажной технологии. Для обеспечения своевременной обработки текущей документации применяется система документооборота, которая позволяет отражать все операции, производимые внутри организации.

Документооборот – это движение документов с момента их получения или создания до завершения исполнения, отправки адресату или сдачи их на хранение.

Организация документооборота на предприятии должна обеспечить: строгий учет поступившей и отправляемой документации; ежедневный контроль по каждому документу за своевременным исполнением; надлежащее хранение входящей и исходящей документации. Модель процесса документооборота представлена на рисунке 3.

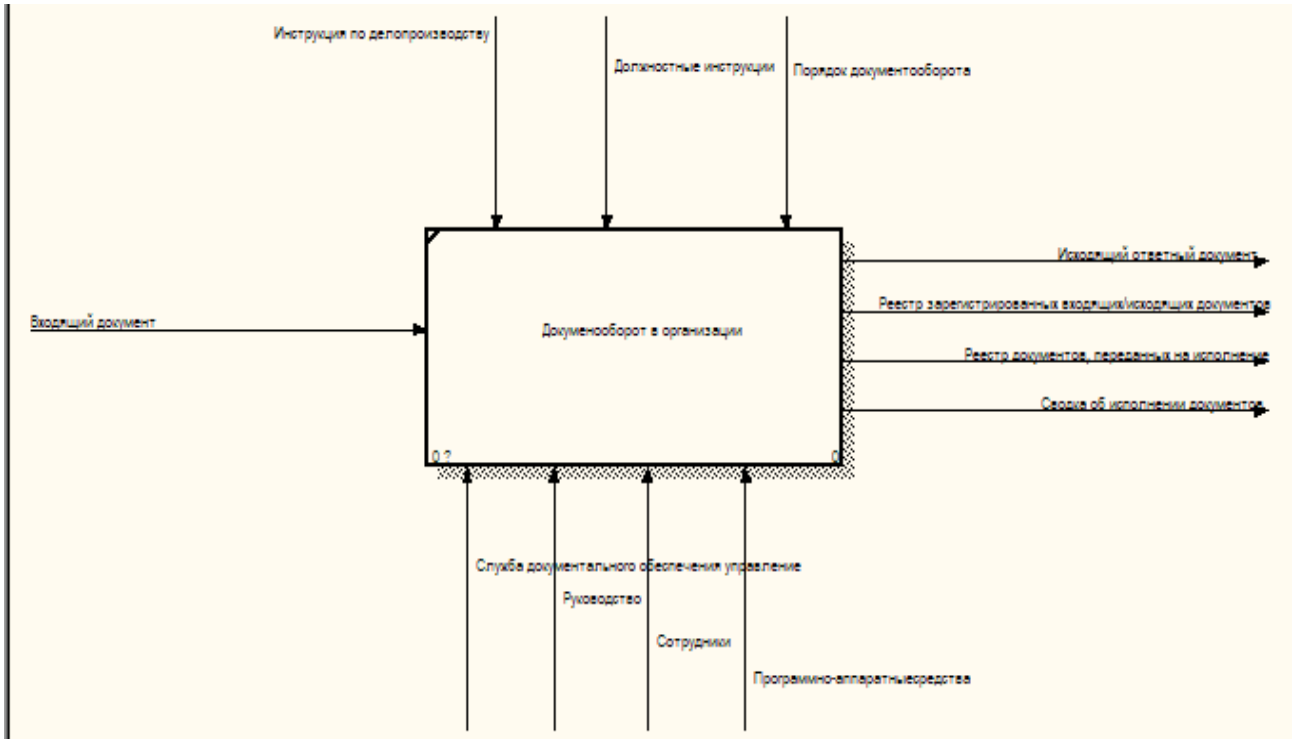

Рисунок 3 – Модель процесса «документооборот в организации»

1.5 Внешний документооборот

Внешний документооборот показывает взаимодействие Центра с внешними объектами. Внешний документооборот представлен на рисунке 4.

Внешними объектами являются:

1 ФЭСТЭК России

2 Управление ФСБ РФ по Амурской области

3 Управление Федеральной налоговой службы РФ

4 УГИБДД УМВД России по Амурской области

5 Медико-санитарная часть МВД РФ

6 Сбербанк России

7 Отделы УМВД России по Амурской области

8 Пенсионный фонд России

9 Прокуратура Амурской области

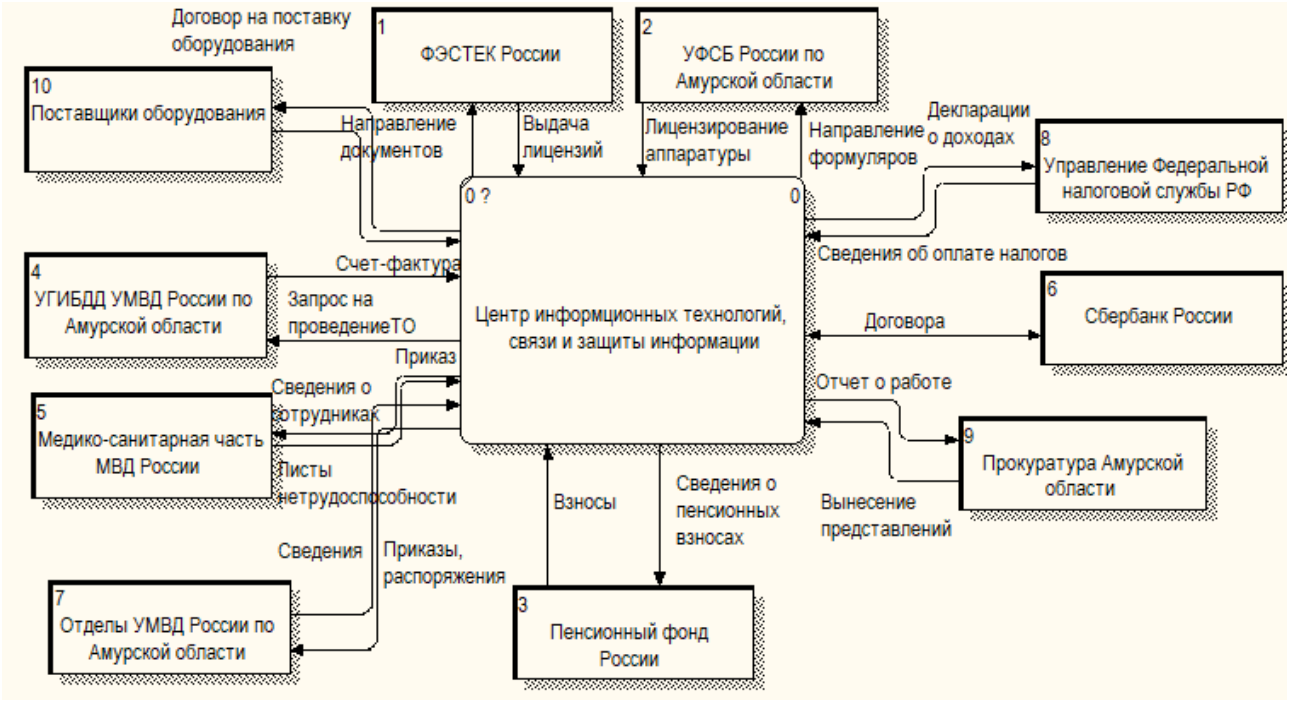

Рисунок 4 – Внешний документооборот ЦИТСиЗИ

1.6 Внутренний документооборот

Внутренний документооборот показывает взаимодействие подразделений Центра информационных технологий, связи и защиты информации УМВД России по Амурской области между собой. Внутренними объектами являются: все структурные подразделения Центра.

Все документы внутри ведомства распределяются в соответствии с функциями подразделений и исполнителей, которые закреплены в положениях о

структурных подразделениях и в должностных инструкциях исполнителей(сотрудников).

Внутренний документооборот объединяет информацию, циркулирующую внутри самого ведомства.

Основными этапами обработки внутренних документов являются:

1 подготовка проекта внутреннего документа;

2 согласования документа;

3 утверждение документа;

4 регистрация документа;

5 рассылка документов по подразделениям;

6 контроль исполнения документа.

Большинство исходящих документов являются ответом организации на соответствующие входящие документы.

К внутренним документам относятся следующие виды документов:

1 организационные (устав организации, должностные инструкции, положения о структурных подразделениях);

2 распорядительные (постановления, распоряжения, приказы);

3 справочно-информационные (акты, анкеты, справки);

4 личные (автобиографии, заявления, доверенности).

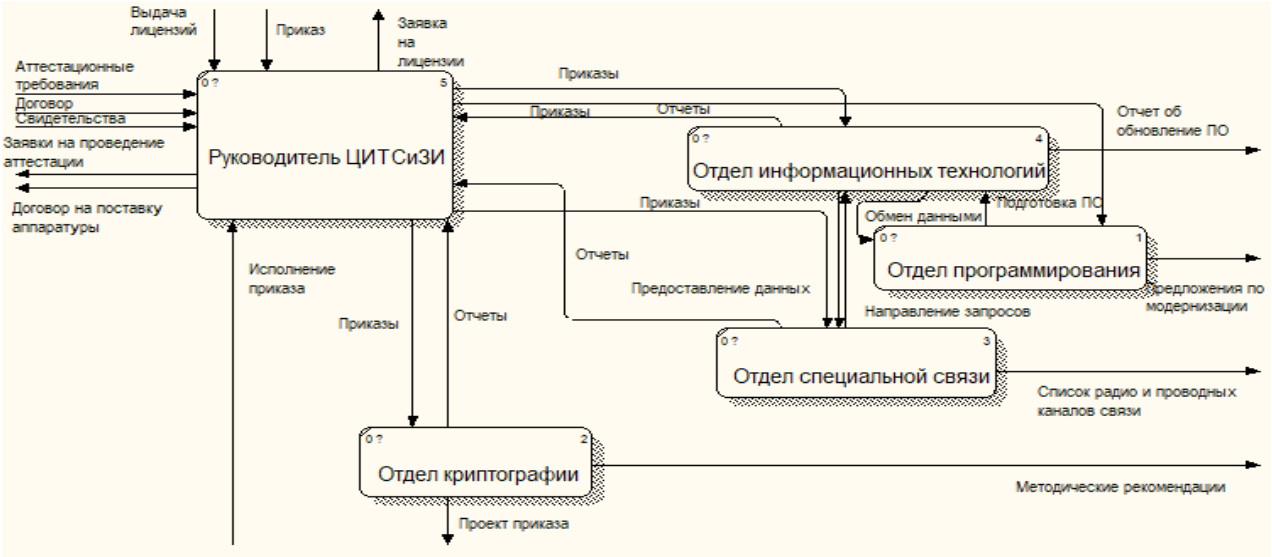

Рисунок 5 – Внутренний документооборот ЦИТСиЗИ

1.7 Объект и предмет защиты

Основными объектами защиты в организации являются:

1 сотрудники Центра;

2 охраняемой законом информацией (государственная тайна, персональные данные) либо имеют доступ в помещения, где эта информация обрабатывается);

3 информационные ресурсы, содержащие конфиденциальную информацию, персональные данные, сведения ограниченного распространения;

4 системы и средства, обрабатывающие конфиденциальную информацию (технические средства приема, обработки, хранения и передачи информации ТСПИ);

5 ТСПИ размещенные в помещениях обработки секретной конфиденциальной информации.

Конфиденциальная информация – это документированная информация, владельцами которой являются государственные, коммерческие и другие организации и учреждения.

Эта информация содержит:

1 сведения, содержащие информацию о персональных данных сотрудников;

2 данные протоколов;

Предметом защиты информации в организации являются носители информации, на которых зафиксированы, отображены защищаемые сведения:

1 бумажный и электронный документооборот;

2 личные дела сотрудников в бумажном и электронном виде;

3 реестр технических средств;

4 другие сведения, относящиеся только для служебного доступа;

5 приказы, положения, постановления, соглашения, инструкции, распоряжения, планы, договоры, отчеты, ведомость ознакомления с положением о конфиденциальной информации и другие документы, в бумажном и электрон-

ном виде.

Документы, которые имеют конфиденциальный характер и требующие защиты:

- материалы кадрового делопроизводства;
- внутренние приказы и распоряжения;
- персональные данные сотрудников;
- схемы информационных потоков и коммуникаций;
- должностные инструкции по отдельным подразделениям;
- активационные коды на лицензионное по;
- архитектура информационной системы;
- приказ о вводе в эксплуатацию ПЭВМ;
- приказ о категорировании и классификации объектов вычислительной техники;
- положение об отделе администрирования и технического сопровождения информационных систем;
- положение о группе инженерно-технической защиты информации;
- положение о структуре службы безопасности;
- положение о компьютерной сети МВД;
- положение об охранно-пропускном режиме УМВД;
- положение об отделе защиты информации;
- должностные инструкции сотрудников предприятия;
- список постоянных пользователей определенного ПЭВМ, допущенных в помещение, и установленные им права доступа к информации и техническим ресурсам ПЭВМ;
- перечень сотрудников ведомства, имеющих доступ к средствам автоматизированной системы (АС) и к обрабатываемой на них информации;
- трудовые договоры сотрудников, работающих с конфиденциальной информацией;

1.8 Угрозы защищаемой информации

Основными угрозами информационной безопасности, возникающими в процессе деятельности оперативно-технических подразделений УМВД.

В настоящее время развитие информационных и телекоммуникационных технологий привело к тому, что современное общество в огромной мере зависит от управления различными процессами посредством компьютерной техники, электронной обработки, хранения, доступа и передачи информации. Согласно информации Бюро специальных технических мероприятий МВД России, в прошлом году было зафиксировано более 14 тыс. преступлений, связанных с высокими технологиями, что немного выше, чем в позапрошлом году. Анализ складывающейся ситуации показывает, что около 16 % злоумышленников, действующих в «компьютерной» сфере криминала, – это молодые люди в возрасте до 18 лет, 58 % – от 18 до 25 лет, причем около 70 % из них имеют высшее либо незаконченное высшее образование.

При этом, 52 % установленных правонарушителей имели специальную подготовку в области информационных технологий, 97 % были сотрудниками государственных учреждений и организаций, использующими ЭВМ и информационные технологии в своей повседневной деятельности, 30 % из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

По неофициальным экспертным оценкам, из 100 % возбуждаемых уголовных дел около 30 % доходят до суда и только 10-15 % подсудимых отбывают наказание в тюрьме. Реальное положение дел по странам СНГ – вопрос из области фантастики. Компьютерные преступления относятся к преступлениям с высокой латентностью, отображающей существование в стране той реальной ситуации, когда определенная часть преступности остается неучтенной.

Серьезную опасность для всего мирового сообщества представляет все более распространяющийся технологический терроризм, составной частью которого является информационный или кибернетический терроризм.

Мишенями террористов становятся компьютеры и созданные на их осно-

ве специализированные системы – банковские, биржевые, архивные, исследовательские, управленческие, а также средства коммуникации – от спутников непосредственного телевещания и связи до радиотелефонов и пейджеров.

Методы информационного терроризма совершенно иные, нежели традиционного: не физическое уничтожение людей (или его угроза) и ликвидация материальных ценностей, не разрушение важных стратегических и экономических объектов, а широкомасштабное нарушение работы финансовых и коммуникационных сетей и систем, частичное разрушение экономической инфраструктуры и навязывание властным структурам своей воли.

Опасность информационного терроризма неизмеримо возрастает в условиях глобализации, когда средства телекоммуникаций приобретают исключительную роль.

В условиях кибернетического терроризма возможная модель террористического воздействия будет иметь «трехступенчатый» вид: первая ступень – это выдвижение политических требований с угрозой в случае их невыполнения парализовать всю экономическую систему страны (во всяком случае, ту ее часть, которая использует в работе компьютерные технологии), вторая – произвести демонстрационную атаку на информационные ресурсы достаточно крупной экономической структуры и парализовать ее действие, а третья – повторить требования в более жесткой форме, опираясь на эффект демонстрации силы.

Отличительной чертой информационного терроризма является его дешевизна и сложность обнаружения. Система Internet, связавшая компьютерные сети по всей планете, изменила правила, касающиеся современного оружия. Анонимность, обеспечиваемая Internetom, позволяет террористу стать невидимым, как следствие, практически неуязвимым и ничем (в первую очередь жизнью) не рискующим при проведении преступной акции.

Положение усугубляется тем, что преступления в информационной сфере, в число которых входит и кибернетический терроризм, влекут за собой наказание существенно меньшее, чем за осуществление «традиционных» тер-

рористических актов. В соответствии с Уголовным кодексом РФ (ст.272, 273), создание программ для ЭВМ или внесение изменений в существующие программы, которые заведомо приводят к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами наказывается лишением свободы на срок максимум до 7 лет. Для сравнения, в США законы карают несанкционированное проникновение в компьютерные сети заключением сроком до 20 лет.

Основой обеспечения эффективной борьбы с кибернетическим терроризмом является создание эффективной системы взаимосвязанных мер по выявлению, предупреждению и пресечению такого рода деятельности. Для борьбы с терроризмом во всех его проявлениях работают различные антитеррористические органы. Особое внимание борьбе с терроризмом уделяют развитые страны мира, считая его едва ли не главной опасностью для общества.

Угрозы информационной безопасности страны, источниками которых являются современная преступность, преступные национальные и транснациональные сообщества, по своей совокупности и масштабам воздействия охватывающие всю территорию страны и затрагивающие все сферы жизнедеятельности общества, обусловливают необходимость рассмотрения борьбы между организованной преступностью и призванными ей противостоять правоохранительными органами, прежде всего, органами внутренних дел, как информационную войну, основной формой ведения которой и ее специфическим содержанием являются информационная борьба с использованием информационно-вычислительных и радиосредств, средств радиотехнической разведки, информационно-телекоммуникационных систем, включая каналы космической связи, геоинформационных систем и иных информационных систем, комплексов и средств.

В условиях современного состояния преступности обеспечить информа-

ционную безопасность в деятельности органов внутренних дел невозможно только на основе применения защитных средств и механизмов. В этих условиях необходимо вести активные наступательные (боевые) действия с использованием всех видов информационного оружия и других наступательных средств в целях обеспечения превосходства над преступностью в информационной сфере.

Появление и развитие новых масштабных явлений в жизни страны и общества, новых угроз национальной безопасности со стороны преступного мира, в распоряжении которого находится современное информационное оружие, и новых условий осуществления оперативно-служебной деятельности органов внутренних дел, определяемых потребностями ведения информационной войны с национальной и транснациональной в своей основе организованной преступностью, обусловливают необходимость соответствующего законодательного, государственно-правового регулирования отношений в сфере информационной безопасности государства в целом и органов внутренних дел в частности.

К основным мероприятиям государственно-правового характера по обеспечению информационной безопасности, осуществляемым, в том числе, и органами внутренних дел, предлагается отнести: формирование режима и охраны в целях исключения возможности тайного проникновения на территорию размещения информационных ресурсов; определение методов работы с сотрудниками при подборе и расстановке персонала; проведение работы с документами и документированной информацией, включая разработку и использование документов и носителей конфиденциальной информации, их учет, исполнение, возврат, хранение и уничтожение; определение порядка использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации; создание технологии анализа внутренних и внешних угроз конфиденциальной информации и выработки мер по обеспечению ее защиты; осуществление систематического контроля за работой персонала с конфиденциальной информацией, порядком учета, хранения и уничтожения документов и технических носителей.

Анализ действующего российского законодательства в области информационной безопасности и государственной системы защиты информации позволяет выделить важнейшие полномочия органов внутренних дел в сфере обеспечения информационной безопасности государства: отражение информационной агрессии, направленной против страны, комплексная защита информационных ресурсов, а также информационно-телекоммуникационной структуры государства; недопущение и разрешение международных конфликтов и инцидентов в информационной сфере; предупреждение и пресечение преступлений и административных правонарушений в информационной сфере; защита иных важных интересов личности, общества и государства от внешних и внутренних угроз.

Правовая защита информации, как ресурса, признана на международном и государственном уровнях. На международном уровне она определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту. На государственном же уровне правовая защита регулируется государственными и ведомственными актами.

К основным направлениям развития российского законодательства в целях защиты информации органов внутренних дел целесообразно отнести:

– законодательное закрепление механизма отнесения объектов информационной инфраструктуры органов внутренних дел к критически важным и обеспечение их информационной безопасности, включая разработку и принятие требований к техническим и программным средствам, используемым в информационной инфраструктуре этих объектов;

– совершенствование законодательства об оперативно-розыскной деятельности в части создания необходимых условий для проведения оперативно-розыскных мероприятий в целях выявления, предупреждения, пресечения и раскрытия компьютерных преступлений и преступлений в сфере высоких технологии; усиления контроля за сбором, хранением и использованием органами внутренних дел информации о частной жизни граждан, сведений, составляю-

щих личную, семейную, служебную и коммерческую тайны; уточнения состава оперативно-розыскных мероприятий;

- усиление ответственности за преступления в сфере компьютерной информации и уточнение составов преступлений с учетом Европейской конвенции о кибернетической преступности;
- совершенствование уголовно-процессуального законодательства в целях создания условий для правоохранительных органов, обеспечивающих организацию и осуществление оперативного и эффективного противодействия преступности, осуществляемого с использованием информационно-телекоммуникационных технологий для получения необходимых доказательств.

Организационно-управленческие меры являются решающим звеном формирования и реализации комплексной защиты информации в деятельности органов внутренних дел.

При обработке или хранении информации органам внутренних дел в рамках защиты от несанкционированного доступа рекомендуется проведение следующих организационных мероприятий: выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите; определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено; установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам защиты; ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации; получение от объекта доступа расписки о неразглашении доверенной ему конфиденциальной информации.

В соответствии с Законом Российской Федерации «О полиции», к компетенции МВД России отнесены функции по формированию общегосударственных справочно-информационных фондов оперативного и криминалистического

учета. Выполнение этих функций осуществляется информационными и техническими подразделениями служб МВД России во взаимодействии с подразделениями криминальной полиции, полиции общественной безопасности, пенитенциарными учреждениями, другими правоохранительными органами, правительственными учреждениями и организациями, ведающими вопросами общественной безопасности, а также правоохранительными органами (полицией) иных государств.

Информационное взаимодействие в сфере борьбы с преступностью ведется в рамках законов Российской Федерации «Об оперативно-розыскной деятельности», «О безопасности», «Об учетах и учетной деятельности в правоохранительных органах», действующих уголовного и уголовно-процессуального законодательства, международных соглашений МВД России в сфере обмена информацией, Положения о МВД России, приказов Министра внутренних дел России.

Исследования показали, что концептуальные положения обеспечения информационной безопасности правоохранительных органов должны включать требования к переходу к единой нормативно-правовой базе, регулирующей процессы использования информации в борьбе с преступностью. При этом в системе министерства внутренних дел вместо многочисленной группы ведомственных актов предлагается ввести три группы нормативно-правовых документов по информационному обеспечению: отраслевые, общего пользования; отраслевые, по линиям служб; нормативно-правовую документацию местного уровня управления по локальным прикладным проблемам информационного обеспечения территориального органа внутренних дел.

2 ОПИСАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

2.1 Этапы построения комплексной системы защиты информации для УМВД России по Амурской области

С целью организации эффективной защиты конфиденциальной информации необходимо разработать информационную систему, которая должна осуществлять следующие цели:

1 предотвращать утечку, хищение, утрату, искажение, подделку конфиденциальной информации;

2 предотвращать угрозы безопасности Центра;

3 предотвращать несанкционированные действия по уничтожению, модификации, искажению, копированию, блокированию конфиденциальной информации;

4 предотвращать другие формы незаконного вмешательства в информационные ресурсы и системы, обеспечивать правовой режима документированной информации как объекта собственности;

5 защищать конституционные права граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;

6 сохранять, конфиденциальность документированной информации в соответствии с законодательством.

Планируемые мероприятия должны:

1 способствовать достижению определенных задач;

2 являться оптимальными.

Не должны:

1 противоречить законам;

2 ГОСТам;

3 требованиям руководителя организации;

4 повторять другие действия.

2.2 Комплексная система защиты информации

Комплексная система защиты информации (КСЗИ) предприятия – это комплекс средств и методов, связанных общим целевым назначением и обеспечивающих необходимую эффективность защиты информации организации.

Главной задачей КСЗИ является обеспечение информационной безопасности, устойчивого функционирования организации и предотвращения угроз.

В комплексную систему защиты информации входит:

1 правовая защита:

1.1 наличие в организационных документах, правилах внутреннего трудового распорядка, трудовых договорах, контрактах, заключаемых с сотрудниками, в должностных инструкциях (регламентах) положений и обязательств по защите информации;

1.2 формулирование и доведение до сведения всего штата сотрудников ведомства (в том числе не связанного с защищаемой и охраняемой информацией) положения о правовой ответственности за разглашение информации, несанкционированное уничтожение или фальсификацию документов;

1.3 разъяснение лицам, принимаемым на работу, положения о добровольности принимаемых ими на себя ограничений, связанных с выполнением обязанностей по защите документированной информации.

2 организационная защита:

2.1 организацию охраны, режима, работу с кадрами, с документами;

2.2 использование ТС безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз.

3 инженерно-техническая защита использует такие средства как:

3.1 физические – устройства, инженерные сооружения, организационные меры, исключающие или затрудняющие проникновение к источникам конфиденциальной информации (системы ограждения, системы контроля доступа, запирающие устройства и хранилища);

3.2 аппаратные – устройства, защищающие от утечки, разглашения и от

ТС шпионажа;

3.3 программные средства – средства, охватывающие специальные программы, программные комплексы и системы защиты информации в информационных системах различного назначения и средствах обработки (сбора, накопления, хранения и передачи) данных.

2.3 Назначение и цели разработки информационной системы

Разрабатываемая информационная система «Контроль исполнения поручений» предназначена для своевременного доведения до сотрудников Центра поставленных перед ними задач, контроля исполнения задач в установленные сроки, удаленного руководства и организации рабочего процесса, консультирование сотрудников и уточнение рабочих графиков.

Главной целью разработки информационной системы «Контроль исполнения поручений» является систематизация контроля рабочего процесса Центра.

Данную цель можно декомпозировать на более мелкие, но не менее важные цели:

- создание и редактирование персональных рабочих графиков сотрудников;
- уточнение задач для каждого сотрудника;
- упрощение контроля выполнения задач.

Достижение всех вышеперечисленных целей в конечном итоге приведет к достижению главной цели – информационной системы «Контроль исполнения поручений».

К основным задачам информационной системы можно отнести:

- обеспечение обратной связи с сотрудниками;
- автоматизация рабочих процессов ведомства;
- повышение качества контроля за исполнением задач.

Рассмотрим контекстную диаграмму функций информационной системы «Контроль исполнения поручений», которая представлена на рисунке 6.

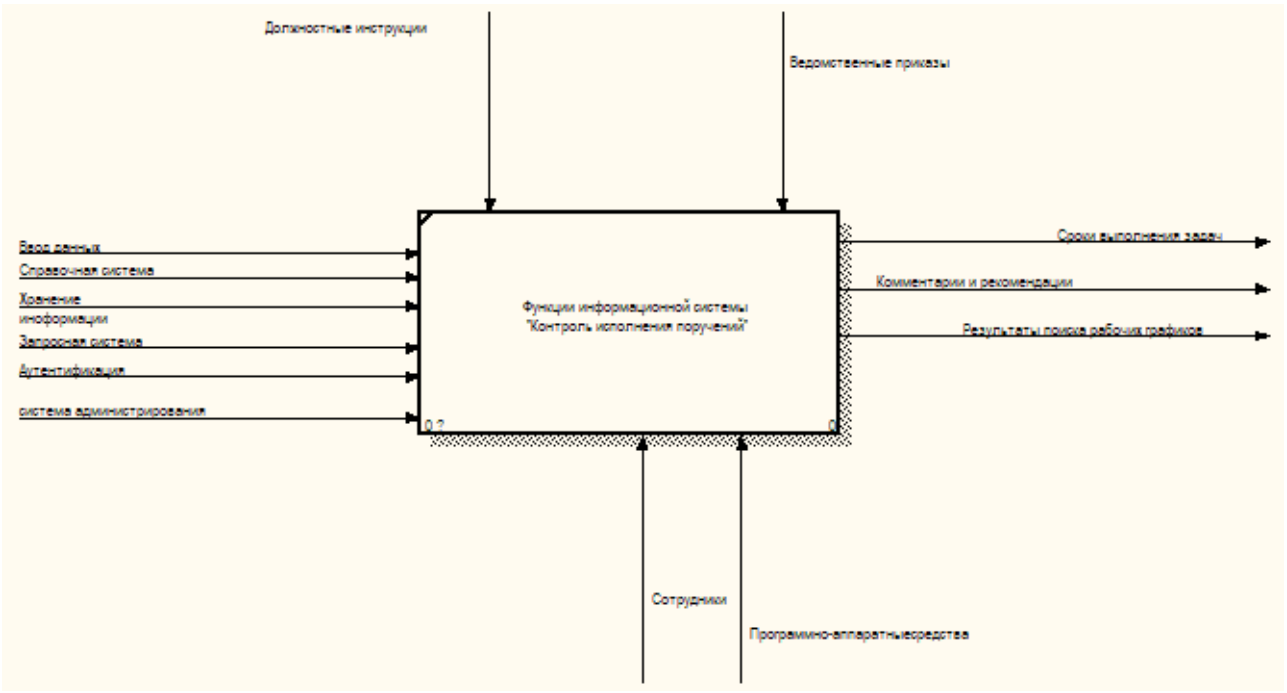

Рисунок 6 – Контекстная диаграмма функций информационной системы «Контроль исполнения поручений»

Информационная система должна выполнять следующие функции:

– информирование об актуальных задачах. В приложении должен быть весь перечень поставленных задач с комментариями и описанием;

– возможность редактировать задачи онлайн. Сотрудник должен иметь возможность уточнить задачу у руководителя;

– возможность оставлять комментарии о проделанной работе;

– возможность осуществлять быстрый поиск по каталогам рабочих графиков, при необходимости, клиент должен иметь возможность найти информацию о той или иной задаче.

Произведем декомпозицию контекстной диаграммы информационной системы для более подробного анализа на рисунке 7.

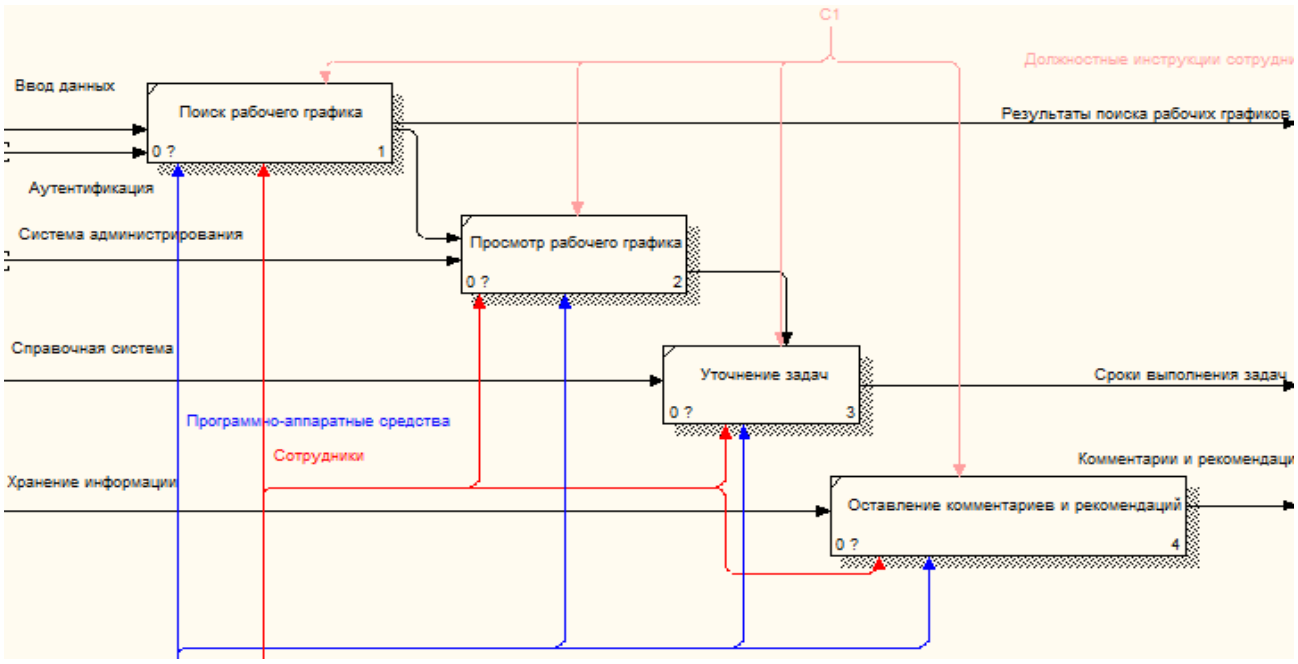

Рисунок 7 – Декомпозиция контекстной диаграммы информационной системы «Контроль исполнения поручений»

Рисунок 8 – Структура информационной системы «Контроль исполнения поручений»

Необходимость создания базы данных обуславливается тем, что она важна для

хранения и получения доступа к информации. Проектирование базы данных заключается в многоступенчатом описании будущей БД с различной степенью детализации и формализации, в ходе, которого производится уточнение и оптимизация ее структуры.

Проектирование включает описание предметной области и задач информационной системы, далее идет к логическому описанию данных и затем – к физической модели БД.

Проектирование баз данных проходит в три этапа:

1 инфологическое проектирование – выделение сущностей и назначение им атрибутов;

2 логическое проектирование – построение логической структуры базы данных, приведение отношений к нормальным формам;

3 физическое проектирование – описываются таблицы в том виде, в котором они реализованы средствами СУБД.

2.4 Инфологическое проектирование

Инфологический подход не содержит формальных способов моделирования реальности, но он закладывает основы методологии проектирования БД.

Первой задачей инфологического проектирования является определение предметной области системы, позволяющее изучить информационные потребности будущих пользователей. Другая задача этого этапа – анализ предметной области, который призван сформировать взгляд на неё с позиций сообщества будущих пользователей БД, инфологической модели предметной области.

Анализ предметной области выполняется проектировщиком БД с помощью специалистов в данной предметной области. В корне анализа лежат документы, используемые в работе предприятия (организации), и технология работы с данными.

Инфологическая модель ПО включает описание структуры и динамики ПО, характера информационных потребностей пользователей системы. Описание выполняется в терминах, понятных пользователю и независимых от реали-

зации системы. Инфологическая модель предметной области не должна зависеть от модели данных, которая будет использована при создании БД.

Как правило описание предметной области выражается в терминах не отдельных сущностей и связей между ними, а их типов, связанных с ними ограничений целостности и тех процессов, которые приводят к переходу предметной области из одного состояния в другое. Такое описание должно быть представлено любым способом, допускающим однозначную интерпретацию.

В простых случаях описание предметной области представляется на естественном языке.

Инфологическое проектирование состоит их нескольких этапов. Первый этап – формирование набора сущностей.

Таблица 1 Наименование сущностей и их описание

Сущность	Описание сущности
«Пользователи»	хранит данные обо всех пользователях, которые работают в компании и имеют доступ к системе.
«Роли пользователей»	хранит данные ролей пользователей, благодаря которым идет разделение доступов к подсистемам.
«Сотрудники»	хранит данные по всем сотрудникам за каким руководителем они закреплены.
«Должности»	хранит данные должностей на предприятии.
«Рабочие графики»	хранит данные запланированного рабочего графика на выполнение по каждому из сотрудников.
«Задачи на день»	хранит данные рабочего графика на день, разбитым на подзадачи (по временному интервалу).
«Статусы задач»	хранит данные возможных статусов для задач.

Второй этап – формирование спецификации атрибутов каждой сущности. Спецификация представлена в таблицах 2-8.

Таблица 2 – Спецификация атрибутов сущности «Пользователи»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
ИД	Уникальный идентификатор пользователя	GUID	-	6F9619FF-8B86-D011-B42D-00CF4FC964FF
Фамилия	Фамилия пользователя	Строка	-	Иванов
Имя	Имя пользователя	Строка	-	Иван
Отчество	Отчество пользователя	Строка	-	Иванович
ИД должности	Уникальный идентификатор должности из сущности «Должности»	GUID	-	0CC11CC3-1F56-4196-BD7F-40B0CE2E7A9B
Дата рождения	Дата рождения пользователя	Дата/Время	-	21.04.1998
Дата приема	Дата приема на работу пользователя	Дата/Время	-	22.05.2021
Пароль	Пароль пользователя для входа в систему (хранится в шифрованном виде MD5)	Строка	-	19f5b3ceaadfd7c0fec5742b9327d6de
Дата создания	Дата добавления пользователя в систему	Дата/Время	-	22.05.2021

Таблица 3 – Спецификация атрибутов сущности «Роли пользователей»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
ИД	Уникальный идентификатор роли	GUID	-	6F9619FF-8B86-D011-B42D-00CF4FC964FF
Название	Наименование роли	Строка	-	Администратор

Таблица 4 – Спецификация атрибутов сущности «Сотрудники»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
ИД	Уникальный идентификатор	GUID	-	132CBCA2-9E5F-4994-9FD2-8ECCB3FCFA39
ИД руководителя	Уникальный идентификатор руководителя	GUID	-	6F9619FF-8B86-D011-B42D-00CF4FC964FF
ИД сотрудника	Уникальных идентификатор сотрудника	GUID	-	06E04BA8-44B5-45AD-B6CE-8EE35CA75E16

Таблица 5 – Спецификация атрибутов сущности «Должности»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
ИД	Уникальный идентификатор должности	GUID	-	0CC11CC3-1F56-4196-BD7F-40B0CE2E7A9B
Название	Наименование должности	Строка	-	Системный администратор

Таблица 6 – Спецификация атрибутов сущности «Рабочие графики»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
ИД	Уникальный идентификатор графика	GUID	-	0B8C459A-0F0F-4A5D-B707-7D822FBF6FB7
ИД пользователя	Уникальный идентификатор пользователя	GUID	-	6F9619FF-8B86-D011-B42D-00CF4FC964FF
Дата выполнения	Дата выполнения указанных задач	Дата/Время	-	25.05.2021

Продолжение таблицы 6

Комментарий	Комментарий к задаче	Строка	-	Задача была выполнена не в срок

Таблица 7 – Спецификация атрибутов сущности «Задачи на день»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
ИД	Уникальный идентификатор подзадачи	GUID	-	073D7D9C-BF27-41AB-9336-74C5EE8F0F9E
ИД рабочего графика	Уникальный идентификатор рабочего графика	GUID	-	0B8C459A-0F0F-4A5D-B707-7D822FBF6FB7
Время начала	Время начала выполнения подзадачи	Время	-	08:00
Время окончания	Время окончания выполнения подзадачи	Время	-	10:00
ИД статуса	Уникальный идентификатор статуса	GUID	-	0066DAC5-7448-44E8-95D3-9C56D3C15C59
Задача	Описание на выполнение подзадачи	Строка	-	Обновить ОС сотруднику в отделе аналитики
Комментарий	Комментарий к подзадаче	Строка	-	Задача перенесена на следующий день

Таблица 8 – Спецификация атрибутов сущности «Статусы задач»

Название атрибута	Описание атрибута	Тип данных	Диапазон значений	Пример атрибута
ИД	Уникальный идентификатор статуса	GUID	-	0066DAC5-7448-44E8-95D3-9C56D3C15C59

Продолжение таблицы 8

Название	Наименование статуса	Строка	-	Выполнено

Третий этап инфологического проектирования – выбор и обоснование первичного ключа, который однозначно идентифицирует каждую запись таблицы.

1 Для сущности «Пользователи» первичным ключом будет являться «ИД», так как такой первичный ключ однозначно идентифицирует сотрудника предприятия.

2 Для сущности «Роли пользователей» первичным ключом будет являться «ИД», так как такой первичный ключ однозначно идентифицирует роль пользователя.

3 Для сущности «Сотрудники» первичным ключом будет являться «ИД», так как такой первичный ключ однозначно идентифицирует связь сотрудников.

4 Для сущности «Должности» первичным ключом будет являться «ИД», так как такой первичный ключ однозначно идентифицирует должность.

5 Для сущности «Рабочие графики» первичным ключом будет являться «ИД», так как такой первичный ключ однозначно идентифицирует рабочий график.

6 Для сущности «Задачи на день» первичным ключом будет являться «ИД».

7 Для сущности «Статусы задач» первичным ключом будет являться «ИД», так как такой первичный ключ однозначно идентифицирует статус задачи.

Четвертый этап – обоснование установления связей. Для получения концептуальной инфологической модели, позволяющей моделировать объекты предметной области и связи между ними, необходимо установить связи между сущностями на основе модели предметной области «сущность-связь».

Назначение модели «сущность-связь» – семантическое описание предметной области и представление информации для обоснования выбора видов моделей и структур данных, которые в дальнейшем будут использованы в системе.

Модель «сущность-связь» предполагает несколько типов связи: «один-к-одному», «один-ко-многим», «многие-ко-многим». Связь «один-к-одному» означает, что в каждый момент времени каждому экземпляру сущности А соответствует 1 и только 1 экземпляр сущности В и наоборот. Связь «один-ко-многим» обозначает, что одному представителю сущности А соответствуют 0, 1 или несколько представителей сущности В, но каждому экземпляру сущности В соответствует только 1 экземпляр сущности А. Связь «многие-ко-многим» показывает, что одному представителю сущности А соответствуют 0, 1 или не сколько представителей сущности В и наоборот.

Таблица 9 – Таблица связей

Название первой сущности, участвующей в связи	Название второй сущности, участвующей в связи	Название связи	Тип связи	Обоснование выбора типа связи
«Пользователи»	«Роли пользователей»	имеют	Один ко многим	Одной записи сущности «роли пользователи» соответствует несколько записей сущности «пользователей» (пр.: Сотрудники – Иванов, Петров, Сидоров)
«Пользователи»	«Должности»	Соответствует	Один ко многим	Каждой записи сущности «должности» соответствует несколько записей сущности «сотрудники», каждой записи сущности «сотрудники» соответствует одна запись сущности «должности»

Продолжение таблицы 9

«Пользователи»	«Сотрудники»	Соответствует	Один ко многим	Каждой записи сущности «Пользователи» соответствует несколько записей сущности «Сотрудники», каждой записи сущности «Сотрудники» соответствует одна запись сущности «Пользователи»
«Пользователи»	«Рабочие графики»	получают	Один ко многим	Каждой записи сущности «пользователи» соответствует несколько записей сущности «рабочие графики»,
«Рабочие графики»	«Задачи на день»	получают	Один ко многим	Каждой записи сущности «Рабочие графики» соответствует несколько записей сущности «Задачи на день», каждой записи сущности «задачи на день» соответствует одна запись сущности «Рабочие графики»
«Задачи на день»	«Статус задач»	Соответствует	Один ко многим	Каждой записи сущности «Задачи на день» соответствует одна запись сущности «Статус задач», каждой записи сущности «Статус задач» соответствует несколько записей сущности «Рабочие графики»

Следующий этап формирование справочника задач, который представляется в виде таблицы:

Таблица 10 – Справочник задач

Наименование задачи	Сущности, используемые при решении задачи
Добавление/редактирование данных пользователя	«Пользователи», «Должности» и «Роли пользователей»
Добавление/редактирование данных должности	«Должности»
Добавление/редактирование данных ролей пользователей	«Роли пользователей»
Добавление/редактирование данных рабочих графиков	«Пользователи», «Рабочие графики», «Задачи на день» и «Статусы задач»
Добавление/удаление сотрудников для руководителя	«Пользователи» и «Сотрудники»

Последний этап – построение инфологической модели БД, которое позволяет обеспечить интегрированное представление о предметной области. Моделирование локального представления заканчивается графическим представлением всех выявленных сущностей, связей между ними и атрибутов с использованием любой из известных нотаций.

Таблица 11 – Наименование сущностей и их описание

Сущность	Описание сущности
«Пользователи»	хранит данные обо всех пользователях, которые работают в компании и имеют доступ к системе.
«Роли пользователей»	хранит данные ролей пользователей, благодаря которым идет разделение доступов к подсистемам.
«Сотрудники»	хранит данные по всем сотрудникам за каким руководителем они закреплены.
«Должности»	хранит данные должностей на предприятии.
«Рабочие графики»	хранит данные запланированного рабочего графика на выполнение по каждому из сотрудников.
«Задачи на день»	хранит данные рабочего графика на день, разбитым на подзадачи (по временному интервалу).
«Статусы задач»	хранит данные возможных статусов для задач.

2.5 Логическое проектирование

Логическая модель базы данных – понимание предметной области в виде данных и связей между ними, преобразованное для эффективной реализации в среде конкретной СУБД.

Связь «пользователи – роли пользователей» является связью типа «Один ко многим». При отображении ключ порожденной сущности добавляется в исходную сущность. Порожденной сущностью является сущность «пользователи», исходной – «роли пользователей».

Сущность «пользователи»

ID пользователя	Фамилия	Имя	Отчество	Дата рождения	Дата приема на работу

Сущность «роли пользователей»

ID роли пользователей	ID статус пользователя	ID пользователя	ID Задачи на день	ID Статус задач

Рисунок 9 – Связь пользователи – роли пользователей

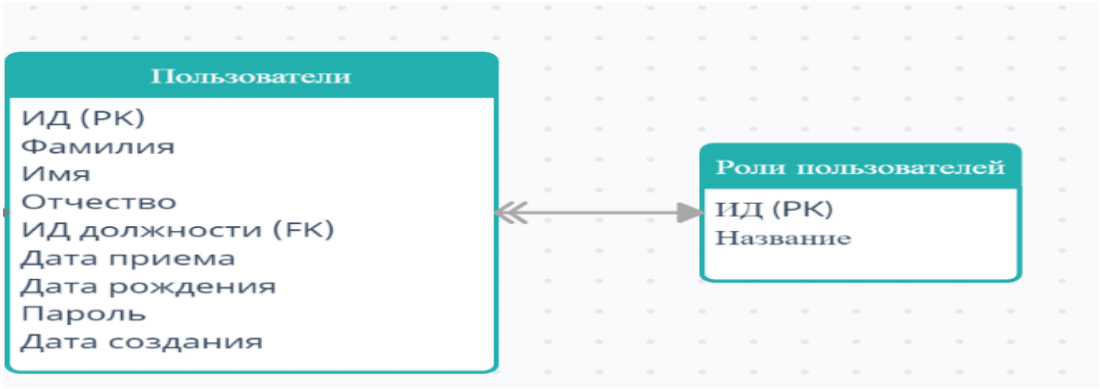

Рисунок 10 – Связь «пользователи – роль пользователей»

Рисунок 11 – Связь «должности – пользователи»

Связь «пользователи – рабочие графики» является связью типа «Один ко многим». При отображении ключ порожденной сущности добавляется в исходную сущность. Порожденной сущностью является сущность «пользователи», исходной – «рабочие графики».

Сущность «пользователи»

ID пользователя	Фамилия	Имя	Отчество	Дата рождения	Дата приема на работу

Сущность «рабочие графики»

ID рабочие графики	ID пользователя	ID Задачи на день	ID Статус задач

Рисунок 12 – Связь «пользователи – Рабочие графики»

Связь «сотрудники -должность» является связью типа «Один ко многим». При отображении ключ порожденной сущности добавляется в исходную сущность. Порожденной сущностью является сущность «сотрудники», исходной – «должность».

Сущность «сотрудники»

ID сотрудник	Фамилия	Имя	Отчество	Дата рождения	Дата приема на работу

Сущность «должность»

ID должность	должность

Рисунок 13 – Связь «сотрудник – должность»

Связь «сотрудник – рабочие графики» является связью типа «Один ко многим». При отображении ключ порожденной сущности добавляется в исходную сущность. Порожденной сущностью является сущность «сотрудники», исходной – «рабочие графики»

Сущность «сотрудник»

ID сотрудник	Фамилия	Имя	Отчество	Дата рождения	Дата приема на работу

Сущность «рабочие графики»

ID рабочие графики	ID сотрудника	ID Задачи на день	ID Статус задач

Рисунок 14 – Связь «сотрудник – рабочие графики»

Связь «сотрудники – задачи на день» является связью типа «Один ко многим». При отображении ключ порожденной сущности добавляется в исходную сущность. Порожденной сущностью является сущность «Задачи на день», исходной – «сотрудники»

Сущность «сотрудники»

ID сотрудники	Фамилия	Имя	Отчество	Дата рождения	Дата приема на работу

Сущность «задачи на день»

ID задачи на день	ID статус задач	задачи

Рисунок 15 – Связь «сотрудники – задачи на день»

Связь «рабочие графики – задачи на день» является связью типа «Один ко многим». При отображении ключ порожденной сущности добавляется в исходную сущность. Порожденной сущностью является сущность «задачи на день», исходной – «рабочие графики».

Рисунок 16 – Связь «рабочие графики – статус задач»

Соответствие отношений трем нормальным формам. Приведение к первой нормальной форме:

Все ключевые атрибуты отношений, полученные на этапе отображения концептуальной инфологической модели на реляционную модель, являются простыми, следовательно, соответствуют первой нормальной форме.

Каждое сформированное отношение удовлетворяет данному условию.

Приведение ко второй нормальной форме:

Отношения находятся во второй нормальной форме, когда они находятся в первой нормальной форме, в них отсутствуют составные ключи и каждый атрибут, который не является основным, функционально полно зависит от ключа.

Поскольку в созданных отношениях отсутствуют составные ключи и все дополнительные атрибуты функционально зависят от первичного ключа, можно утверждать, что все отношения приведены ко второй нормальной форме.

Приведение к третьей нормальной форме:

Проанализировав отношения, можно сделать вывод, что они находятся в третьей нормальной форме, так как они находятся во второй нормальной форме и все атрибуты, которые не являются ключевыми, не имеют транзитивной зависимости от ключевых атрибутов.

2.6 Физическое проектирование

Физическое проектирование является третьим и последним этапом создания проекта базы данных и заключается в расширении ее логической модели такими характеристиками, которые необходимы, во-первых, для определения способов физического хранения и использования базы данных и, во-вторых, для определения объемов памяти, требуемой для всей системы и для оценки эффективности обработки. Подобные характеристики касаются того, как и где хранить данные, как их можно найти и использовать.

Таблица 12 – Спецификация атрибутов сущности «Пользователи»

Название атрибута	Тип данных	Условие	Формат данных	Индексация
Id	GUID	-	uniqueidentifier	Primary key
Login	Текст	NOT NULL	nvarchar(16)	Unique
FirstName	Текст	NOT NULL	nvarchar(32)	-
MiddleName	Текст	NOT NULL	nvarchar(32)	-
LastName	Текст	NOT NULL	nvarchar(32)	-
PositionId	GUID	NOT NULL	uniqueidentifier	Foreign Key
DateBirthday	Дата/Время	NOT NULL	datetime	-
EmploymentDate	Дата/Время	NOT NULL	datetime	-
Password	Текст	NOT NULL	nvarchar(512)	-
RoleId	GUID	NOT NULL	uniqueidentifier	Foreign Key
Created	Дата/Время	-	datetime	-
Modified	Дата/Время	-	datetime	-

Таблица 13 – Спецификация атрибутов сущности «Роли пользователей»

Название атрибута	Тип данных	Условие	Формат данных	Индексация
Id	GUID	-	uniqueidentifier	Primary key
Name	Текст	NOT NULL	nvarchar(32)	Unique

Таблица 14 – Спецификация атрибутов сущности «Сотрудники»

Название атрибута	Тип данных	Условие	Формат данных	Индексация
Id	GUID	-	uniqueidentifier	Primary key
LeaderId	GUID	NOT NULL	uniqueidentifier	-

Продолжение таблицы 14

WorkerId	GUID	NOT NULL	uniqueidentifier	-

Таблица 15 – Спецификация атрибутов сущности «Должности»

Название атрибута	Тип данных	Условие	Формат данных	Индексация
Id	GUID	-	uniqueidentifier	Primary key
Name	Текст	NOT NULL	nvarchar(32)	Unique

Таблица 16 – Спецификация атрибутов сущности «Рабочие графики»

Название атрибута	Тип данных	Условие	Формат данных	Индексация
Id	GUID	-	uniqueidentifier	Primary key
UserId	GUID	NOT NULL	uniqueidentifier	Foreign Key
DateOfWork	Дата/Время	NOT NULL	datetime	-
Comment	Текст	-	nvarchar(512)	-
Created	Дата/Время	-	datetime	-
Modified	Дата/Время	-	datetime	-

Таблица 17 – Спецификация атрибутов сущности «Задачи на день»

Название атрибута	Тип данных	Условие	Формат данных	Индексация
Id	GUID	-	uniqueidentifier	Primary key
OperatingGraphId	GUID	NOT NULL	uniqueidentifier	Foreign Key
TimeStart	Текст	Формат «00:00»	nvarchar(5)	-
TimeEnd	Текст	Формат «00:00»	nvarchar(512)	-
StatusTaskId	GUID	NOT NULL	uniqueidentifier	Foreign Key
Comment	Текст	-	nvarchar(512)	-
Description	Текст	-	nvarchar(512)	-
Created	Дата/Время	NOT NULL	datetime	-
Modified	Дата/Время	-	datetime	-

Таблица 18 – Спецификация атрибутов сущности «Статусы задач»

Название атрибута	Тип данных	Условие	Формат данных	Индексация
Id	GUID	-	uniqueidentifier	Primary key
Name	Текст	NOT NULL	nvarchar(32)	Unique

2.7 Руководство 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.

К программе предъявляются следующие требования к надежности:

1 Система должна содержать идентификацию всех пользователей;

2 Система должна обеспечивать надежное хранение данных;

3 Система должна предотвращать несанкционированный доступ к данным.

К работе с информационной системой имеют доступ все сотрудники организации. Руководитель организации, сотрудники, которые работают с информационной системой, и системный администратор, который следит за работоспособностью системы и в случае ошибок системы исправляет их.

Пароль для авторизации должен быть назначен не менее восьми символов. Обязательным условием является наличие в пароле заглавных и строчных букв, цифр и символов. Логин от трех до двадцати символов.

Для работы с системой необходимо запустить программу. После запуска появится форма авторизации пользователя. Вход в систему для каждого сотрудника осуществляется под индивидуальными данными.

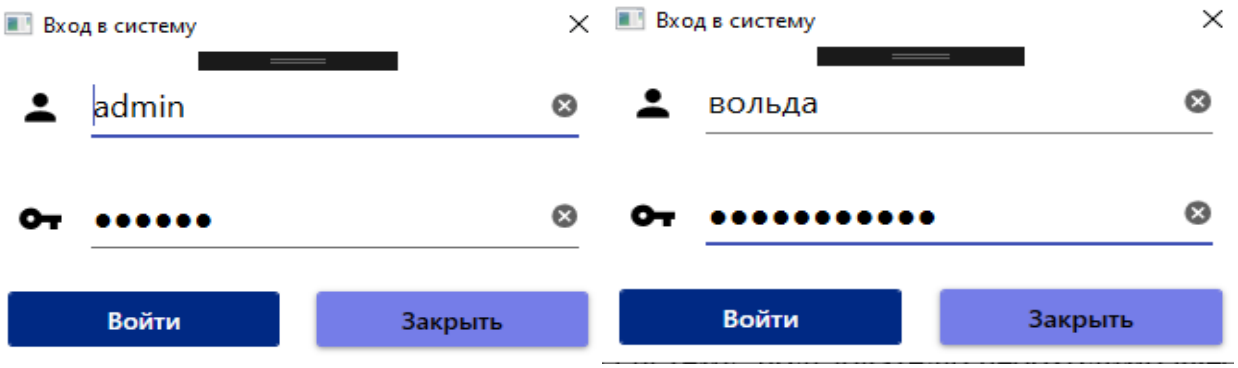

Рисунок 17 – Экранная форма авторизации

Чтобы войти в систему, пользователю необходимо ввести логин и пароль в поле ввода и нажать кнопку «Войти» для начала работы в системе. Логин и пароль у каждого сотрудника индивидуален и должен изменяться каждые 3 месяца. Остальные сотрудники или посторонние не могут знать и обладать логином и паролем. В случае, когда сотрудник вводит неверные логин или пароль появляется сообщение об ошибки (рисунок 18), после клика мышью на кнопку ОК» откроется окно авторизации для повторного входа в систему.

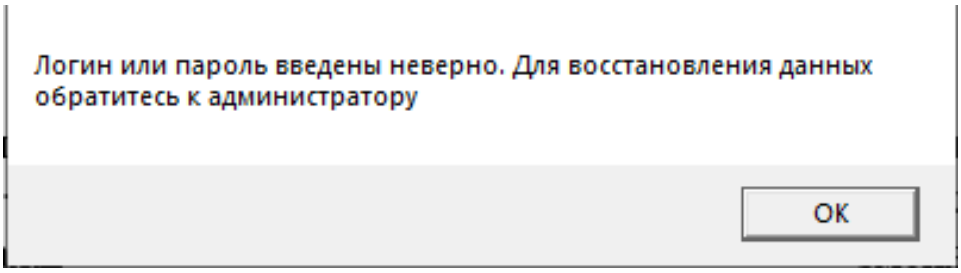

Рисунок 18 – Окно ошибки

После прохождения процедуры авторизации пользователю открывается главная экранная форма работы с системой. Для каждого пользователя, в зависимости от должности, свой набор функций.

Для поддержания бесперебойной работоспособности данной системы необходим системный администратор, который отвечает за модернизации, настройку и мониторинг работоспособности комплекса технических средств, в случае поломки. Экранные формы пользователей показаны на рисунках 19-24.

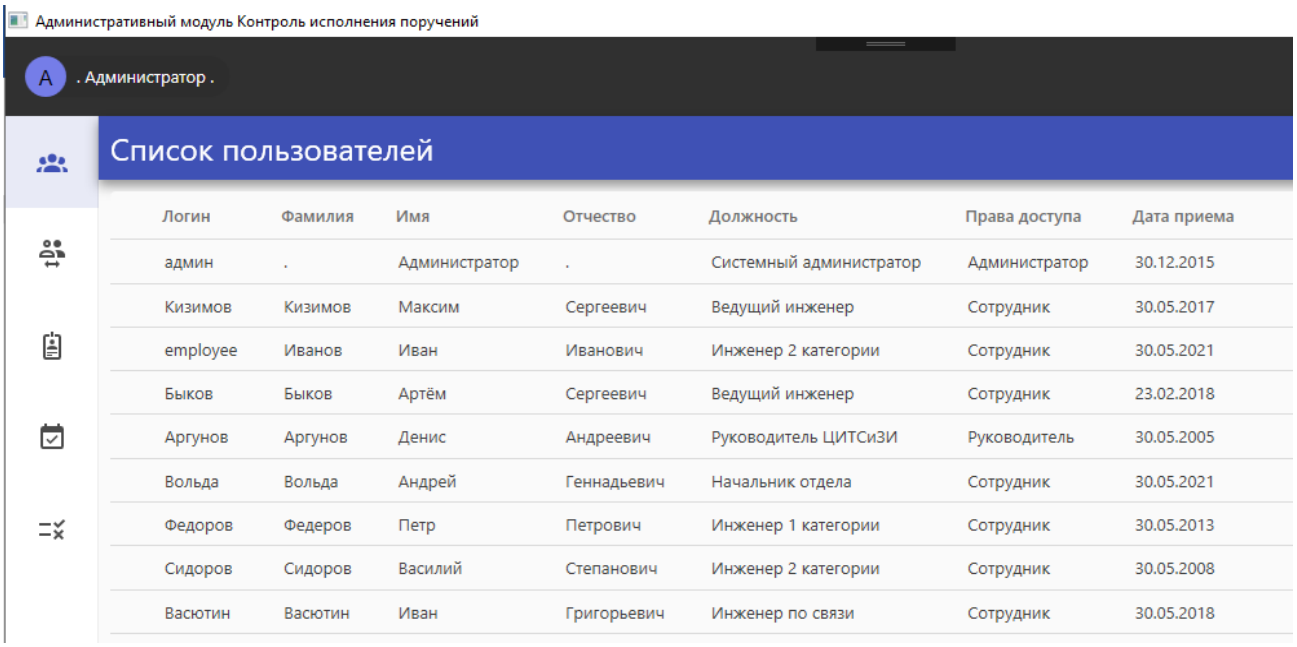

Рисунок 19 – Главная экранная форма пользователя – Администратора

Администратор является полноправным пользователем АРМ и обладает следующими возможностями:

- добавления пользователей АРМ
- ограничения прав пользования
- восстановления пароля
- редактирования задач, календарных планов
- устанавливать отметки о выполнении
- изменять интерфейс
- изменять исходные коды программы
- изменять личные данные сотрудников.

АРМ Руководителя организации включает в себя следующие функции:

1 восстановления пароля

2 постановка задач и установление времени их выполнения

3 оставлять комментарии к календарным графикам и задачам

4 просматривать отчет о выполнении поставленных задач

5 фильтровать по дате, ФИО исполнителя

6 удалять и редактировать задачи- возможность составления рабочего графика, как для себя, так и для своих сотрудников

7 возможность просмотра личных данных.

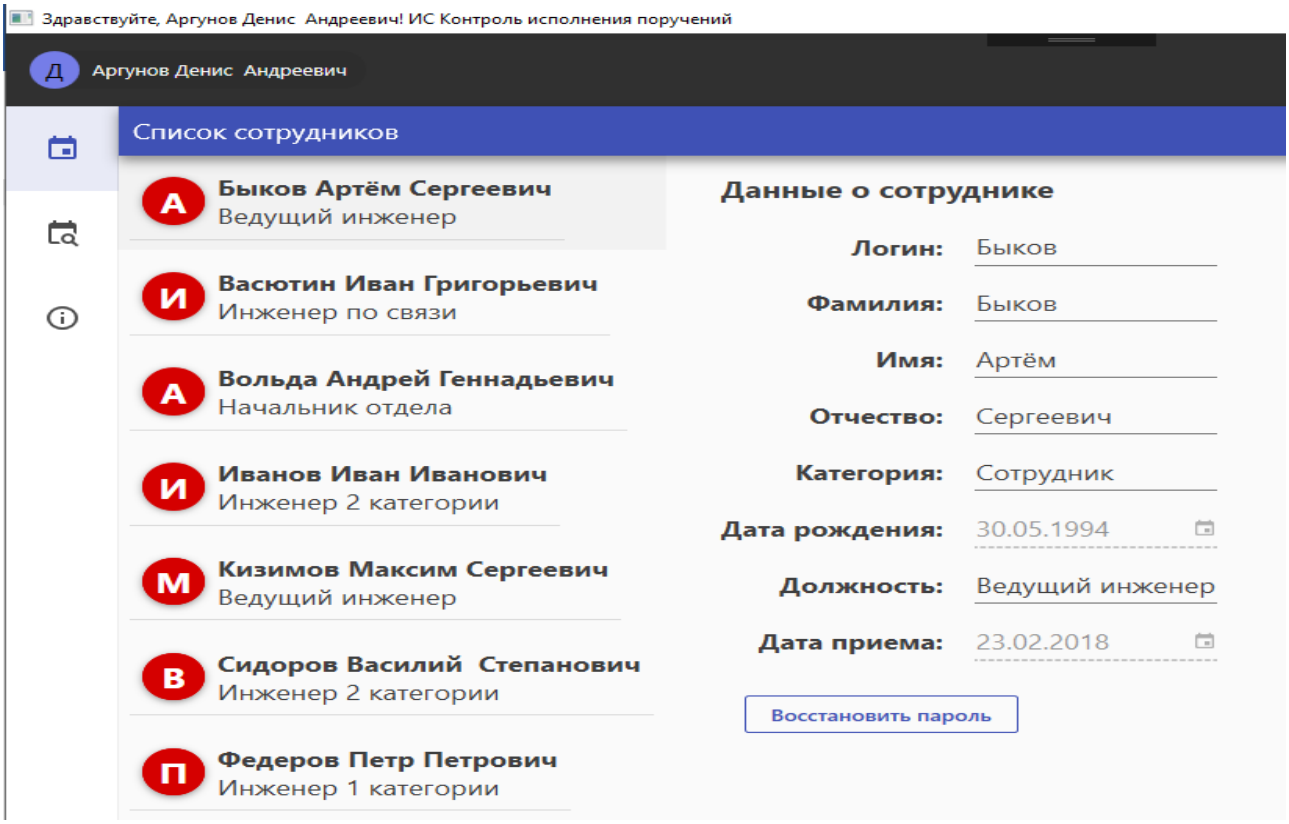

Рисунок 20 – Экранная форма пользователя – Руководителя

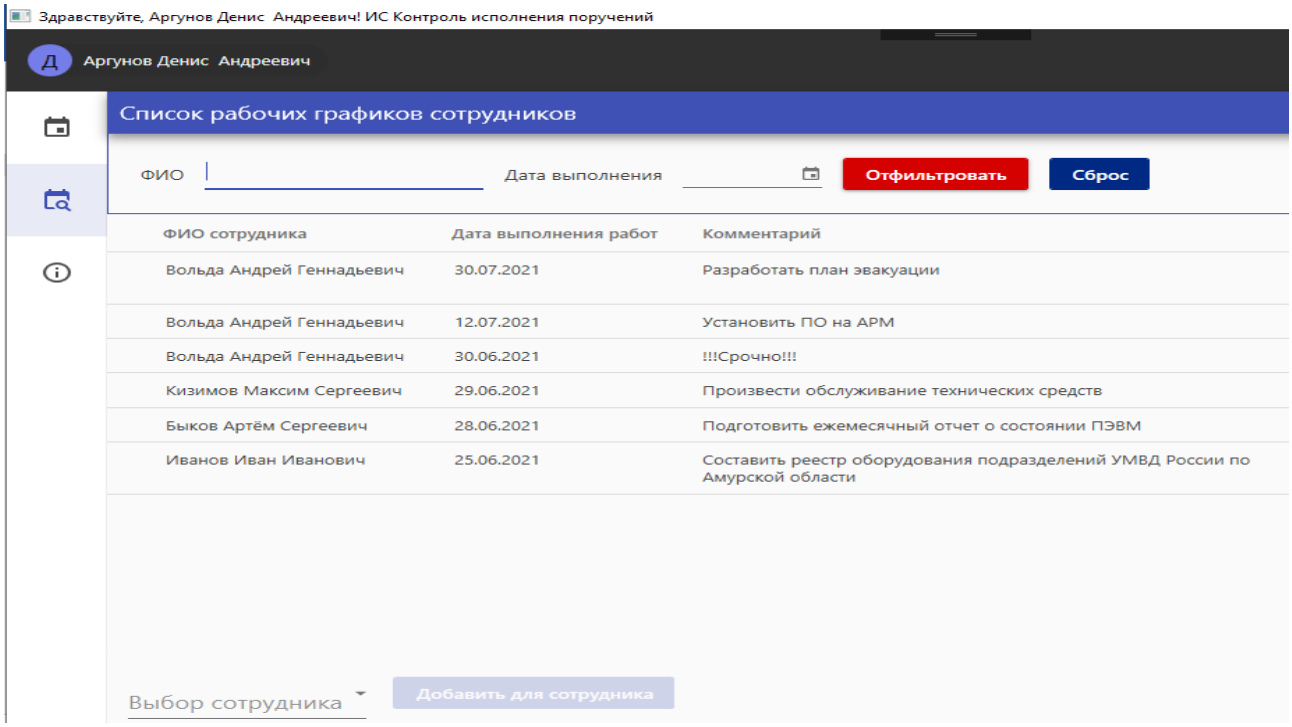

Рисунок 21 – Экранная форма – Список рабочих графиков сотрудников

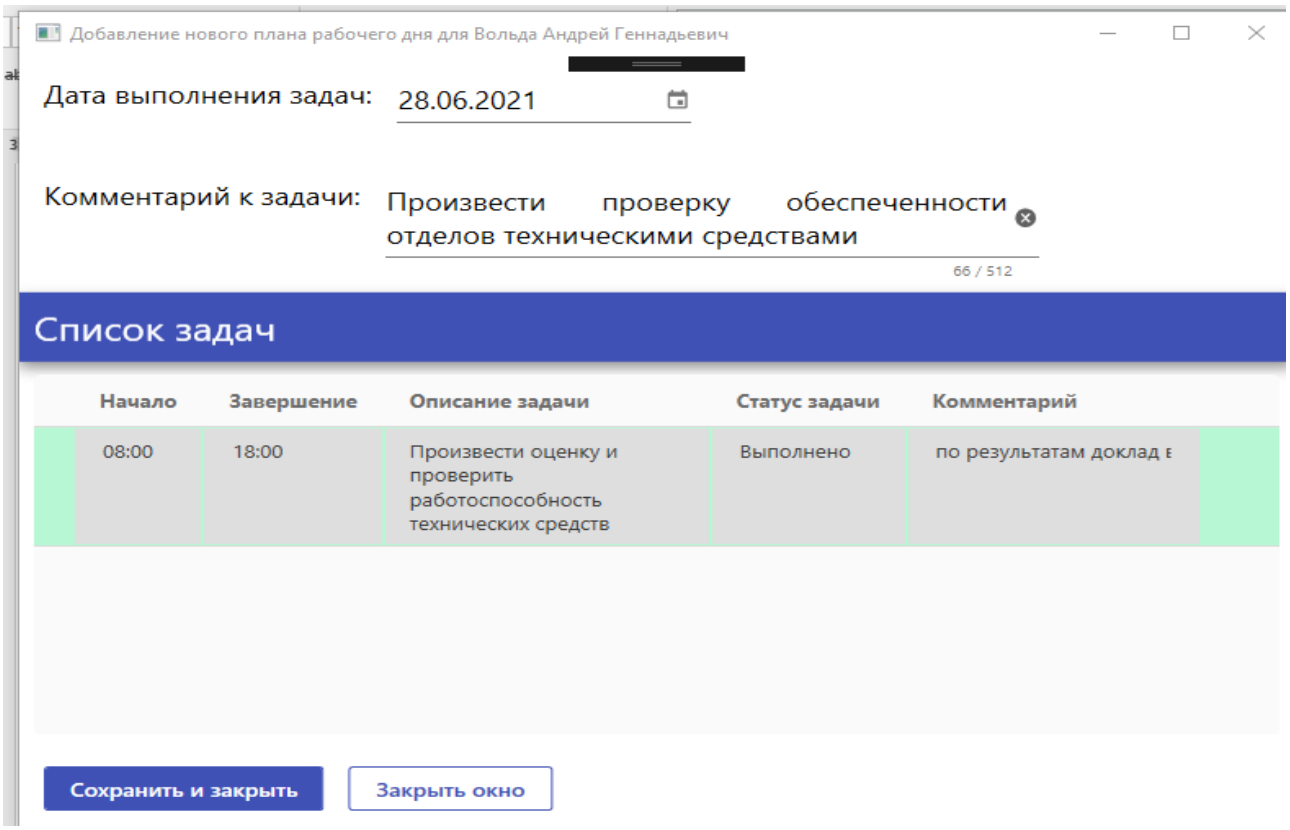

Рисунок 22 – Экранная форма – добавление задачи сотруднику

Личный кабинет пользователя – Сотрудник имеет доступ к следующим функциям:

1 просмотр поставленных задач

2 добавление комментария к задаче

3 поддерживать связь с руководителем

4 возможность составления личного рабочего графика на последующие рабочие дни (без возможности редактирования)

5 возможность выставления статусов о проделанных работах по составленному графику на текущую дату

6 возможность просмотра личных данных

7 возможность изменения пароля.

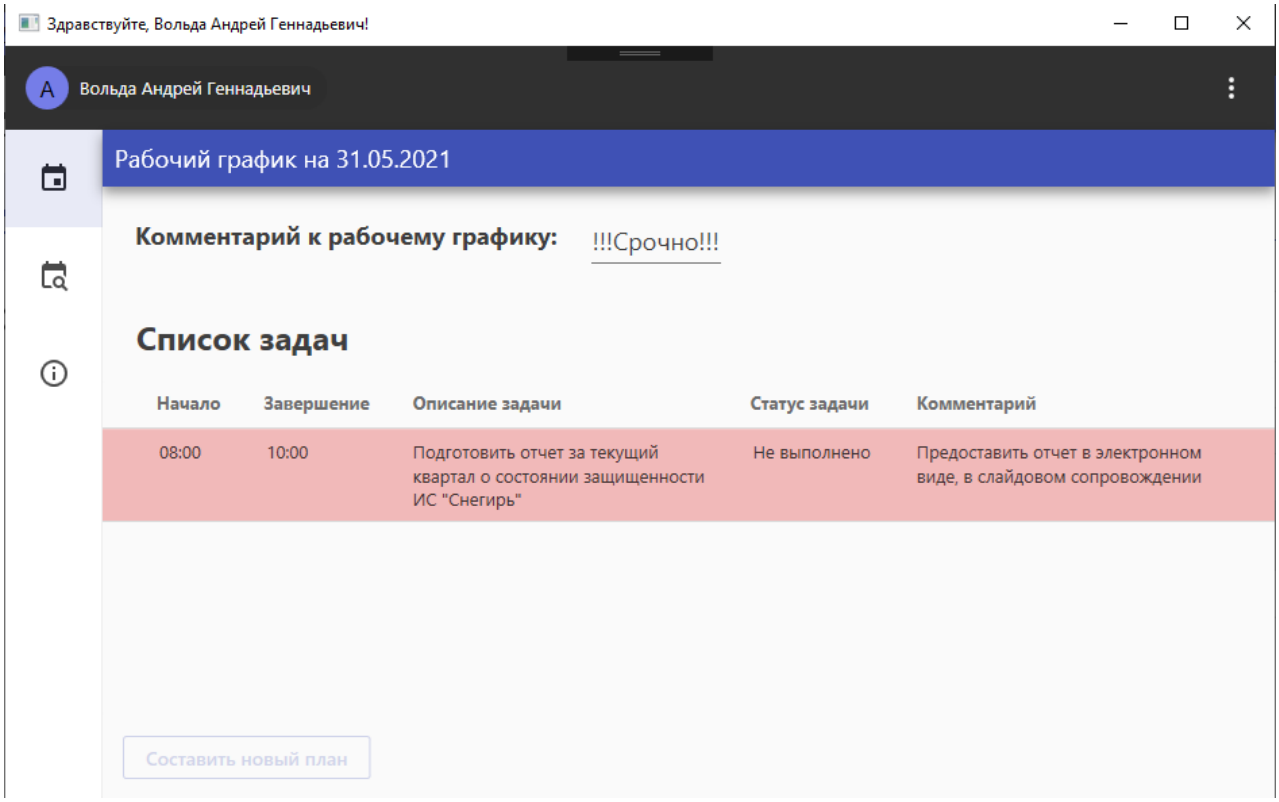

Рисунок 23 – Экранная форма пользователя – Сотрудника

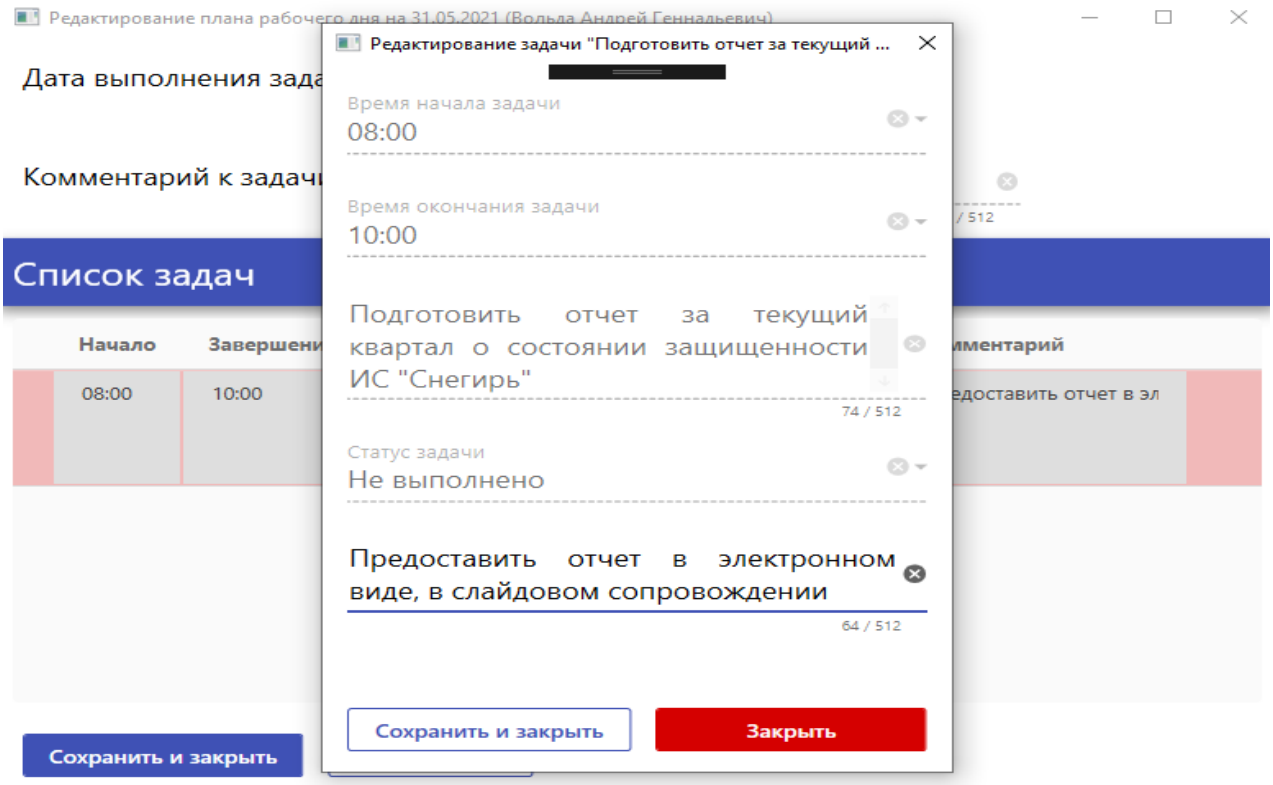

Рисунок 24 – Экранная форма – Добавление комментария к задаче

Пользователи обязаны быть проинформированы о правилах использования технических средств и работы с программой и с оборудованием, на кото-

ром используется данная программа.

Исследовав данную программу, можно выделить такие достоинства, как простота использования, легкий интерфейс, информативное меню, широкий спектр решаемых задач, сведены к минимуму риски несанкционированного доступа, неограниченный функционал.

С целью реализации данной программы разработано техническое задание (приложение А)

В полной мере программный интерфейс представлен в приложении Б.

3 ИНФОРМАЦИОННАЯ СИСТЕМА ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ МВД РОССИИ КАК СОВРЕМЕННЫЙ ЭТАП РАЗВИТИЯ ЕДИНОЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЫ

В марте 2012 года МВД РФ утвердило концепцию создания единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России в 2012-2014 гг. Она представляет собой совокупность используемых в министерстве автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, а также систем связи и передачи данных, необходимых для обеспечения служебной деятельности ведомства.

Создание ИСОД стало продолжением проекта единой информационно-телекоммуникационной системы (ЕИТКС) ОВД, который велся с 2005 года. Важнейшей составной частью этой системы являлась телекоммуникационная подсистема, обеспечивающая информационное взаимодействие всех подразделений ОВД с другими правоохранительными органами и госорганами различных уровней.

Основной причиной принятия решения о создании ИСОД в материалах структур МВД называется отсутствие единых архитектурных решений и системного подхода к внедрению автоматизированных систем в ведомстве.

В процессе создания ИСОД должны быть решены задачи автоматизации основных видов деятельности подразделений МВД, организации централизованного хранения и обработки данных. По задумке МВД, система должна стать единым источником информации для всех сотрудников подразделений МВД, служить для организации электронного взаимодействия между ними, обеспечения разграниченного доступа к информационным ресурсам.

В ведомстве также рассчитывают, что создание ИСОД будет способствовать повышению эффективности принимаемых решений за счет улучшения качества подготавливаемых отчетов, основанных на актуальных и достоверных

данных, обеспечения оперативного и своевременного анализа ключевых показателей деятельности МВД России.

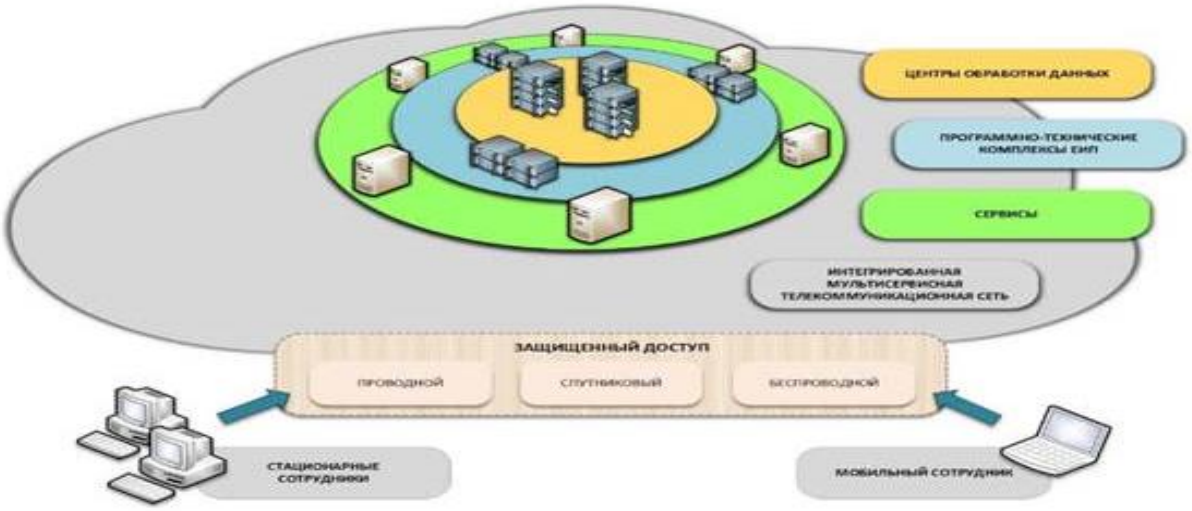

Рисунок 25 – Структура ИСОД МВД России

ИСОД МВД России — это совокупность используемых в МВД России автоматизированных систем обработки информации, программно-аппаратных комплексов и программно-технических средств, систем связи и передачи данных.

Цель создания ИСОД — повышение уровня информационно-аналитического обеспечения МВД России.

Одним из основных требований к подсистеме безопасности ИСОД МВД России является использование современных методов защиты информации с возможностью адаптации к возникающим вызовам и угрозам информационной безопасности, а также своевременное выявление угроз «нулевого дня» и предотвращение атак типа «человек посередине».

Основа построения ИСОД предусматривает создание центров обработки данных (ЦОД), а также реализацию облачной архитектуры (виртуализации) на базе создаваемых ЦОД. Это добавляет новые технологии и требует привлечения дополнительных специализированных мер и средств защиты информации.

Основной элемент инфраструктуры ИСОД — Единая информационная система централизованной обработки данных (ЕИС ЦОД), которая создается на

нескольких территориально удаленных площадках. Это необходимо для обеспечения требуемых уровней показателей надежности и доступности.

Доступ пользователей к ресурсам централизованных информационных систем МВД России возможен с автоматизированных рабочих мест или ведомственных мобильных устройств.

В ЦОДе планируется использовать серверы на процессорах «Эльбрус».

За счет создания ЕИС ЦОД в МВД рассчитывают унифицировать используемые в ведомстве программно-технические решения и привести архитектуру основных автоматизированных информационных систем в соответствие современным требованиям к доступности и надежности. Он должен обеспечить консолидацию разнородных данных, содержащихся в различных системах МВД и обеспечить единую точку доступа к ним для использования в оперативно-служебной деятельности МВД.

В числе ожидаемых эффектов от создания ЦОДа – уменьшение расходов на создание, поддержку и эксплуатацию автоматизированных информационных систем, используемых в МВД.

В 2013 году проводилась ОКР по созданию технологической инфраструктуры ЦОДа. Из ТЗ по этому проекту следует, что вычислительную основу в нем должны составлять, главным образом, серверы IBM, основу для хранения данных – решения EMC.

В результате выполнения ОКР создается образец «Единой системы информационно-аналитического обеспечения деятельности МВД России» в составе:

1 Интегрированная мультисервисная телекоммуникационная сеть (ИМТС);

2 Система централизованной обработки данных (ЦОД и ПТК);

3 Прикладные сервисы обеспечения повседневной деятельности подразделений МВД РФ (Повседневные сервисы ИСОД);

4 Прикладные сервисы обеспечения оперативно-служебной деятель-

ности подразделений МВД РФ (Служебные сервисы ИСОД);

5 Подсистема поддержки взаимодействия подразделений МВД РФ с населением, а также межведомственного взаимодействия;

6 Подсистема обеспечения информационной безопасности (ПОИБ).

Рисунок 26 – Состав сервисов ИСОД МВД России

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД России включают:

1 СЭД – Сервис электронного документооборота;

2 СЭП – Сервис электронной почты;

3 ВИСП – Ведомственный информационно-справочный портал;

4 СВКС-М – Система видеоконференцсвязи МВД России.

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД РФ должны быть внедрены в 85 субъектах РФ.

Прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД РФ включают:

1 Следопыт-М – Информационно-поисковый сервис;

2 СООП – Сервис обеспечения охраны общественного порядка;

3 СОДЧ – Сервис обеспечения деятельности дежурных частей;

4 СОМТО – Сервис обеспечения деятельности подразделений материально-технического обеспечения МВД РФ;

5 ФИС ГИБДД-М – Федеральная информационная система ГИБДД МВД РФ;

6 СОЭБ – Сервис обеспечения экономической безопасности;

7 СОДИ – Сервис НЦБ Интерпола;

8 ЕАИС ЭКП – Сервис экспертно-криминалистической деятельности;

9 СУОГЗ – Сервис обеспечения государственной защиты лиц;

10 СОПС – Сервис оформления проезда сотрудников;

11 СОПД ГУСБ – Сервис ГУ Собственной безопасности МВД;

12 МОСТ – Сервис статистической отчетности МВД РФ;

13 ЦИАДИС-МВД – Банк отпечатков пальцев.

Прикладные сервисы обеспечения повседневной деятельности подразделений МВД РФ должны быть внедрены (пользователи применяют) в 45 субъектах РФ. Состав и количество субъектов уточняется на этапе технического проектирования.

Подсистема поддержки взаимодействия с населением, а также межведомственного взаимодействия с целью предоставления государственных услуг, включает:

1 СПГУ – Сервис предоставления государственных услуг;

2 СЦУО – Система централизованного учета оружия;

3 Ретроспектива – Единый банк данных архивной информации;

4 Модернизация ИБД – Интегрированный банк данных.

Основные требования:

1 Внедрить систему эл. очередей в подразделениях МВД (где закуплено оборудование);

2 Внедрить СПГУ в 85 субъектах РФ;

3 Предложить пути оптимизации и совершенствования оказания государственных услуг.

3.1 Задачи создания СУДИС

Во-первых, требовалось создать единый пополняемый реестр пользователей ИСОД МВД России. При поиске системы, содержащей наибольшее количество данных о сотрудниках МВД России на начало 2014 года, было принято решение осуществить интеграцию с подсистемой организационно-штатной структуры сервиса электронного документооборота (далее ОШС). В результате в настоящее время при появлении новой записи сотрудника МВД России в ОШС автоматически создается учетная запись в реестре пользователей СУДИС с присвоением индивидуальных логина и пароля, а также прав доступа «по умолчанию» к сервисам ИСОД МВД России. При удалении записи из ОШС учетная запись пользователя.

Во-вторых, так как ИСОД МВД России объединяет в себе сервисы, функционирующие на базе как лицензируемого, так и разрабатываемого в интересах МВД России программного обеспечения (далее ПО), нужно было определить перечень программных интерфейсов, с помощью которых сервисы могли бы интегрироваться с СУДИС для обеспечения процессов идентификации и аутентификации пользователей.

В-третьих, разрабатываемое ПО СУДИС должно было поддерживать различные способы аутентификации (проверки подлинности пользователя):

- По логину и паролю — наиболее простой способ, реализуемый вышеуказанными интерфейсами «по умолчанию»;
- С помощью ключа электронной подписи — предпочтительный способ с точки зрения информационной безопасности, но требующий построения полномасштабной инфраструктуры открытых ключей. Для реализации инфраструктуры открытых ключей в системе МВД России создан и функционирует Удостоверяющий центр МВД России. Удостоверяющий центр успешно прошел процедуру аккредитации Минкомсвязи России и выпускает только квалифицированные сертификаты ключей проверки электронной подписи.

В-четвертых, уже на начальных этапах создания СУДИС были разработа-

ны требования к сложности и частоте смены паролей для обеспечения необходимого уровня безопасности, что в некотором роде осложнило жизнь пользователям (учитывая низкий процент использования средств электронной подписи на начало 2014 года). В рамках оптимизации процесса аутентификации пользователей по логину и паролю была внедрена система однократной аутентификации для веб-приложений сервисов ИСОД МВД России. Она позволила пользователю вводить учетные данные только один раз при начале работы в одном из сервисов и автоматически (прозрачно для пользователя) проверяла его подлинность при переходе в другие сервисы в рамках одной рабочей сессии.

Таким образом, на начальном этапе создания ИСОД МВД России сервис управления доступом обеспечил возможности:

1 Ведения единого реестра учетных записей пользователей ИСОД МВД России;

2 Идентификации и аутентификации пользователей в различных типах клиентов сервисов ИСОД МВД России;

3 Входа в сервисы с помощью логина и пароля или ключа электронной подписи;

4 Однократной аутентификации на рабочих местах и в веб-приложениях сервисов ИСОД МВД России.

В настоящее время в СУДИС реализованы механизмы сбора и предоставления статистической отчетности на основании данных об успешных аутентификациях пользователей в сервисах ИСОД МВД России.

События успешной и неуспешной аутентификации пользователей, создания и изменения значимых ресурсов ИСОД МВД России и другие события безопасности регистрируются в сервисе протоколирования событий безопасности СУДИС (далее СПСБ). С учетом интеграции СПСБ со специализированными средствами подсистемы обеспечения информационной безопасности ИСОД МВД России можно смело отметить, что СУДИС делает серьезный вклад в решение задачи обнаружения попыток несанкционированного доступа к инфор-

мационным ресурсам ИСОД МВД России.

Остальные функции СУДИС получили свое развитие относительно недавно и включают следующие механизмы:

1 Механизмы поддержки специализированных типов учетных записей (далее УЗ), помимо управления стандартными УЗ сотрудников МВД России СУДИС позволяет управлять доступом к сервисам ИСОД МВД сотрудников других органов исполнительной власти. При этом на специализированные УЗ распространяются отдельные (более строгие) политики информационной безопасности.

2 Механизмы ограничения доступа пользователей к сервисам ИСОД МВД России по способу входа или типу УЗ, можно, например, разрешить доступ пользователей к конкретному сервису ИСОД МВД России только посредством ключей электронной подписи.

3 Механизмы рассылки уведомлений по электронной почте о событиях, связанных с УЗ пользователей, в настоящее время пользователь ИСОД МВД России, который работает под учетной записью СУДИС, может получать уведомления об истечении срока действия своего пароля или сертификата ключа проверки электронной подписи, а также при изменении полномочий доступа или данных учетной записи администратором безопасности.

3.2 Трудности внедрения

Несмотря на то, что СУДИС в настоящее время реализует достаточно широкий перечень функций, остаются факторы, в некоторой степени препятствующие его быстрому внедрению в подразделениях МВД России. В основном это связано с отсутствием или недостаточным развитием отдельных прикладных решений в ИСОД МВД России, которые в классических корпоративных информационных системах реализуются с помощью коммерческого ПО и удовлетворяют следующие потребности пользователей и администраторов систем:

1 Возможность использования сетевых разделяемых ресурсов (общих

файлов, папок, принтеров и т. п.);

2 Возможность использования специальных функций программного обеспечения, которое функционирует только в рамках домена Microsoft Active Directory (например, совместная работа с документами в программах пакета Microsoft Office);

3 Централизованное управление парком автоматизированных рабочих мест со стороны системных администраторов. СУДИС в той или иной степени может накладывать технические ограничения на использование коммерческого ПО. В частности, он полностью блокирует возможность построения доменов Microsoft Windows на базе Microsoft Active Directory;

4 Еще одним фактором, влияющим на скорость внедрения СУДИС, является отсутствие в ИСОД МВД России полного и корректного (с точки зрения качества информации) источника данных о сотрудниках МВД России и структуре МВД России. Сервисы кадрового учета (Сервис обеспечения кадровой деятельности и Сервис организационно-штатных подразделений) находятся в стадии разработки и пока не предоставляют программных интерфейсов, необходимых для обеспечения доступности кадровых данных. Это приводит, например, к появлению дублей учетных записей и необходимости их выявления и удаления на стороне СУДИС в рамках задачи по обеспечению защиты от несанкционированного доступа.

4 БЕЗОПАСНОСТЬ И ЭКОЛОГИЧНОСТЬ

4.1 Безопасность жизнедеятельности программиста

Трудовая деятельность человека всегда протекает в определенных метеорологических условиях. Метрологические условия формируются с помощью совокупности температуры воздуха, скорости его движения, относительной влажности, барометрическим давлением и тепловым излучением от нагретых поверхностей. В том случае, когда работа выполняется внутри помещений (в изолированном пространстве), соответственно эти показатели в сочетании обозначают микроклиматом производственного помещения.

4.1.1 Требования к ПЭВМ

В соответствии с требованиями допустимые уровни звукового давления и уровней звука, создаваемого ПЭВМ не превышают рекомендуемой нормы.

Временные допустимые уровни электромагнитных полей, создаваемых ПЭВМ, не превышает допустимого диапазона.

Допустимые визуальные параметры устройств отображения информации в норме.

Дизайн и окраска ПЭВМ в соответствии с нормами обладают мягкими тонами, имеют матовую поверхность, как и клавиатура и другие блоки и устройства компьютера, не имеют блестящих деталей.

4.1.2 Требования к помещениям

Освещение должно быть, как искусственным, так и естественным и отвечать всем нормам. Естественное освещение выполнено с помощью оконных проемов. Окна располагают на севере в помещении где сотрудники работают с компьютерами, оборудованы жалюзи. Искусственное освещение реализовывается с помощью светильников и прожекторов. Степень освещения помещения и яркость экрана монитора компьютера должны быть примерно одинаковыми, потому что яркий свет в районе периферийного зрения значительно увеличивает напряженность глаз, что приводит к их быстрой утомляемости. В помещении

каждый день проводится влажная уборка и проветривание помещения. Также помещение оборудовано защитным заземлением для обеспечения безопасности сотрудников. Температура внутри помещения колеблется от 22 ºС до 25 ºС, размещен кондиционер для регулирования температуры воздуха внутри помещения.

Согласно требованиям, в помещение уровень вибрации и шума не превышает допустимые значения. Для предотвращения пожаров, помещение оборудовано средствами пожаротушения, а именно огнетушителями, установлены датчики дыма и пожарная сигнализация. Имеется план эвакуации из помещения, где работают сотрудники, назначен ответственный за пожарную безопасность. Для поддержания нормального микроклимата необходим достаточный объем вентиляции, для чего в помещении должны быть учтены системы отопления, вентиляции и кондиционирования, независимо от наружных условий, и в теплое, и в холодное время года.

4.1.3 Организация рабочего места

Рабочие столы размещены так, чтобы мониторы были расположены боковой стороной к оконным проемам. Площадь на одно рабочее место составляет 6 м2 исходя из расчетов площади помещения 12 м 2. Схема расположения рабочих мест представлена на рисунке 20.

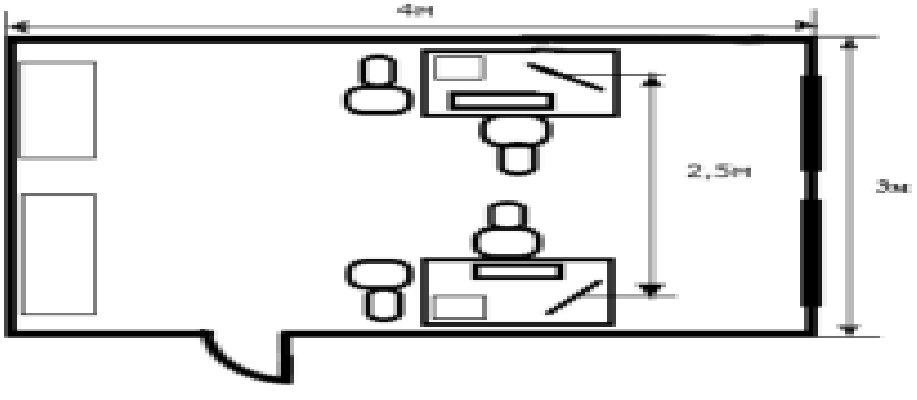

Рисунок 27 – Схема расположения рабочих мест

Высота рабочей поверхности составляет 728 мм, что удовлетворяет требованиям. Размеры и форма сидений и спинки стула полумягкие, с нескользя-

щими и слабо электризующимся и воздухопроницаемым покрытием, что позволяет легко очистить от загрязнений также соответствует нормам, а угол наклона спинки – регулируемый. Подходящая высота сиденья над уровнем пола находится в пределах 420-550мм. а угол наклона спинки – регулируемый.

На рабочем месте сотрудников размещены дисплей, клавиатура и системный блок. При включении дисплея на электронно-лучевой трубке создается высокое напряжение в несколько киловольт. В связи с этим запрещается прикасаться к тыльной стороне дисплея, вытирать пыль с компьютера при его включенном состоянии, работать на компьютере во влажной одежде и влажными руками.

Рабочая поза сидя вызывает минимум утомления сотрудника. Благоразумная планировка рабочего места предусматривает правильный порядок и постоянство размещения предметов, средств труда и документации. То, что требуется для выполнения работ чаще, расположено в зоне легкой досягаемости рабочего пространства.

На рисунке 28 представлены зоны досягаемости рук в горизонтальной плоскости.

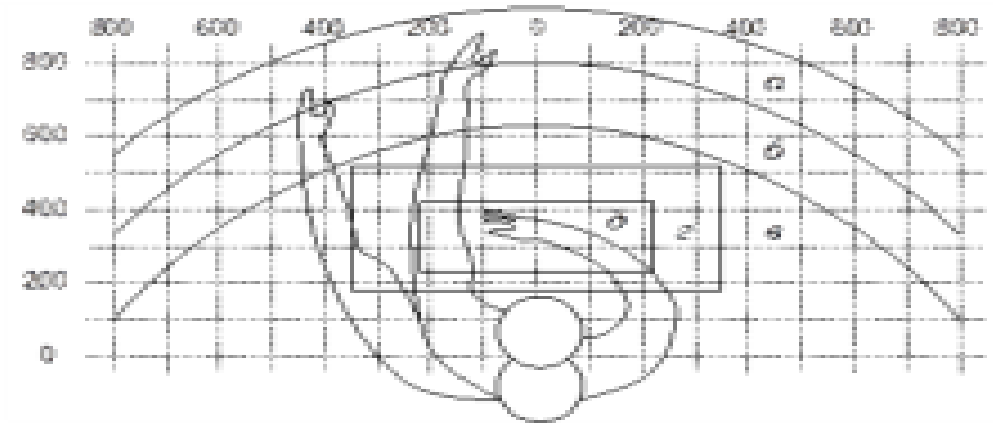

Рисунок 28 – Зоны досягаемости рук в горизонтальной плоскости (зона а – максимальной досягаемости, зона б – досягаемости пальцев при вытянутой руке, зона в – легкой досягаемости ладони, зона г – оптимальное пространство для грубой ручной работы, зона Д – оптимальное пространство для тонкой ручной работы)

Оптимальное размещение предметов труда и документации в зонах досягаемости:

– дисплей размещается в зоне а (в центре);
– системный блок размещается в предусмотренной нише стола;
– клавиатура – в зоне г/д;
– «мышь» – в зоне в справа;
– сканер – в зоне а/б (слева);
– принтер – находится в зоне а (справа).

4.1.4 Требования к эргономичности программного продукта

Для точного восприятия информации и обеспечения комфортных условий работа проводится при сочетании яркости, контраста изображения, внешней освещенности экрана, угла наблюдения экрана, которые входят в допустимые диапазоны.

Для чтения текса применяется синий и черный цвета символов и знаков. Число цветов, одновременно отображаемых на экране дисплея минимально, а именно для точной идентификации цвета используется пять цветов, что удовлетворяет нормам. Для быстрого поиска, основанного на распознавании цветов, применятся три цвета.

Для точного распознавания и идентификации цветов применяется цветное изображение.

Для лучшего восприятия обычным пользователем применяется удобное расположение полей для ввода информации, а после и вывода информации. На рисунке 29 представлен пример интерфейса программного продукта.

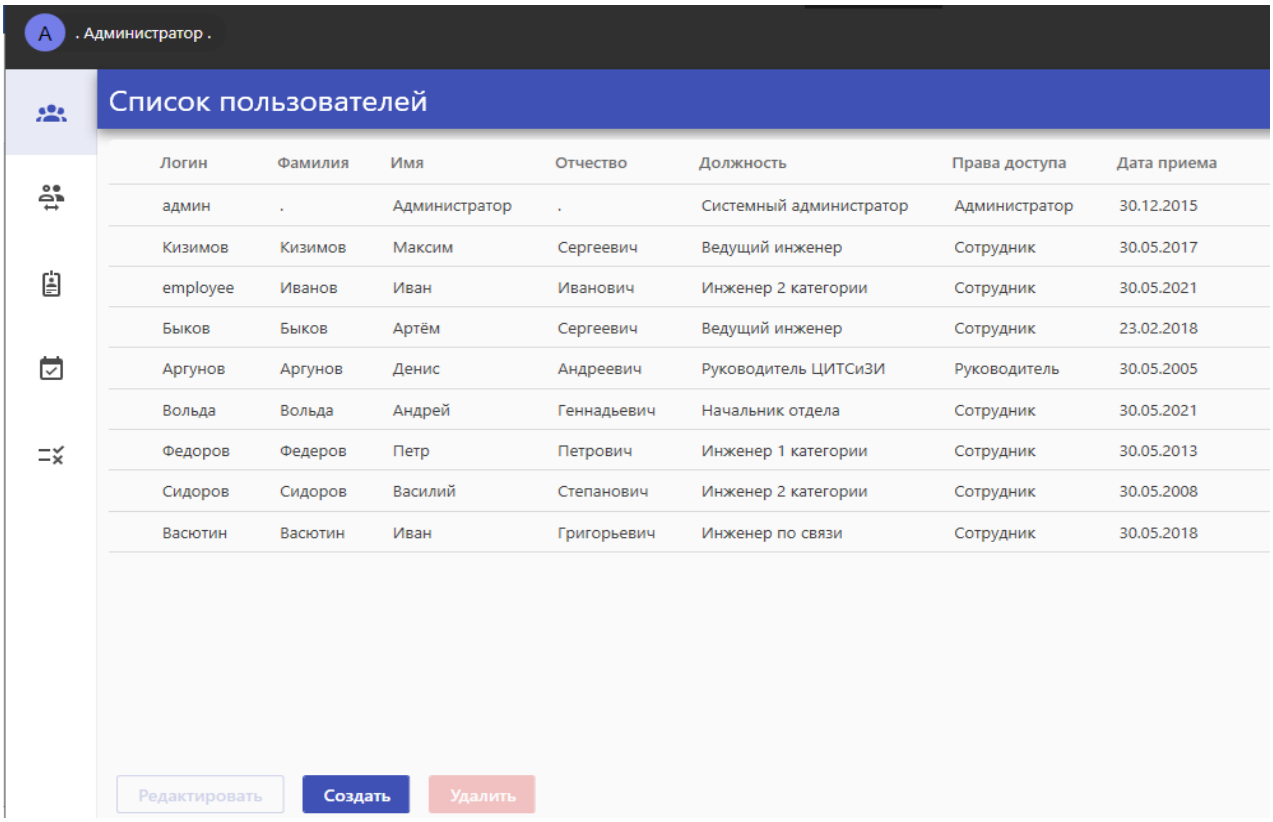

Рисунок 29 – Интерфейс программного продукта

4.2 Экологичность

Экологичность отходов – это свойства отходов, которые представляют естественную или обеспеченную способность при всех видах существования не оказывать отрицательные воздействия на окружающую среду.

Для обеспечения экологичности на рабочих местах необходимо проанализировать методы утилизации в Организации бумажных отходов, компьютерной техники и оргтехники, ламп освещения.

4.2.1 Утилизация бумажных отходов

Первым шагом для организации утилизации бумажных отходов является найти фирму приемщик. В городе Благовещенск этой работой занимается открытое акционерное общество «Вторичные ресурсы». Далее руководство Организации обговаривает условия для сбора макулатуры и заключение договора. В Организации создается приказ об организации сбора вторичного сырья. Выделяется место для сбора вторичного сырья. После всех мероприятий, когда собирается необходимое количество вызывается машина и загружается. На пункте

приема машину взвешивают и выписывают необходимые документы.

4.2.2 Утилизация компьютерной техники и оргтехники

ПЭВМ состоит из компонентов, которые содержат в себе токсичные вещества и которые представляют угрозу для сотрудников, а также для окружающей среды.

К таким веществам относятся:

– ртуть (этот элемент поражает мозг и нервную систему), находится в мониторах, сканер-копир;

– никель и цинк (эти элементы могут вызывать дерматит), находится в материнской плате и батареях питания для ноутбуков;

– щелочи (эти элементы прожигают слизистые оболочки и кожу), находятся в щелочных аккумуляторах источников бесперебойного питания;

– поливинилхлорид (эти элементы разрушает нервную систему и вызывает раковые заболевания), находится в кабелях, которые подключаются к электронным устройствам.

Поэтому ПЭВМ требует особенных комплексных методов утилизации. Руководство подготавливает список оргтехники, подлежащей утилизации. Следующим шагом становится отправка этого самого списка в компанию, занимающееся утилизацией, для того, чтобы компания могла ознакомится со списком и установить стоимость. Далее подписывается договор между организациями и вызывается техника для погрузки не рабочей техники. Далее происходит непосредственно утилизация Первым делом разбирается техника и сортируются ее компоненты на лом черных и цветных металлов, платы с драгоценными металлами, пластик и отходы, которые е подлежат переработке. После полученное сырье передается на заводы по переработке, а остальные отходы обезвреживаются и подвергаются уничтожаются. По завершении разборки компьютера на компоненты, заказчику предоставляют акт об утилизации.

4.2.3 Утилизация ламп

В Организации используют люминесцентные лампы для общего освеще-

ния помещения и энергосберегающие лампы для настольного освещения.

Утилизация начинается с заключением договора на обслуживание с организацией. Далее производится сбор ламп. Лампы хранятся в специальной таре. И не реже, чем раз в полгода, отправляют на переработку. Транспортировка осуществляется в герметичной таре и на специальном транспорте.

Для этого стеклянные части колбы поступают в измельчитель, где происходит измельчение стекла с нанесенным на него люминофором до определенной фракции. После этого осуществляется сдувание люминофора потоком сжатого воздуха. Далее, его частицы поступают в контейнер, где нагреваются до температуры кипения ртути. Полученная газообразная ртуть конденсируется на охлаждаемых конденсаторах. В результате производственного цикла получают отдельно тяжелый металл и сопутствующие вещества, такие как стекло и составляющие люминофора. Это дает возможность последующего их использования.

4.3 Чрезвычайные ситуации

4.3.1 Требования электробезопасности

При использовании средств вычислительной техники и периферийных устройств сотрудники должны внимательно и осторожно обращаться с электропроводкой, приборами и аппаратами. Чтобы избежать поражения электрическим током необходимо знать и правильно применять правила безопасного пользования электроэнергией. Необходимо следить за исправным состоянием электропроводки, выключателей, розеток, с помощью которых в сеть включается оборудование, и заземления. В случае обнаружения неисправности необходимо обесточить электрооборудование и оповестить руководство, работу можно продолжать только после устранения неисправности.

Во избежание поражения электрическим током запрещено часто включать и выключать компьютер, прикасаться к экрану и тыльной стороне блоков компьютера, с мокрыми руками работать на средствах вычислительной техники и периферийном оборудовании, при нарушении целостности корпуса, наруше-

ния изоляции проводов, с признаками электрического напряжения н корпусе, при неисправной индикации включения питания работать на средствах вычислительной техники и периферийном оборудовании, а также запрещено класть посторонние вещи на средства вычислительной техники и периферийном оборудовании.

Во избежание повреждения изоляции проводов и возникновения коротких замыканий запрещено закрашивать и белить шнуры и провода, вешать что-либо на провода, выдергивать штепсельную вилку из розетки за шнур (усилие должно быть приложено к корпусу вилки).

Во всех случаях, когда человека поражает электрическим током без замедления, вызывают скорую помощь. Тем временем, до прибытия скорой помощи пострадавшему оказывают первую помощь.

4.3.2 Требования по обеспечению пожарной безопасности

Чтобы избежать чрезвычайной ситуации в виде пожара, на рабочем месте запрещено зажигать огонь, включать электрооборудование, если в помещении присутствует запах газа, сушить что-то на отопительных приборах, закрывать вентиляционные отверстия в электрооборудовании.

Если возникла пожароопасная ситуация или пожар, то необходимо принять меры по его ликвидации, а также оповестить о этой ситуации руководство. Для обеспечения пожарной безопасности помещения должны быть оборудованы огнетушителями углекислотными, порошковыми или пенными. Помещение должно быть оснащено автоматической системой газового пожаротушения, для повышения безопасности рекомендуется установить противопожарные дымовые датчики. Чтобы избежать паники среди сотрудников и быстрой безопасной эвакуации у дверных проемов, выключателей, рубильников, по пути возможной эвакуации следует размещать фотолюминесцентные эвакуационные знаки. В качестве дополнительных мер для звукоизоляции и акустической отделки стен и потолков необходимо применять несгораемые материалы. Источники электрической энергии необходимо располагать в обособленных помещениях. Для

хранения важных бумаг, переносных носителей информации применяют в оборудованных стеллажах из негорючих материалов. Система электропитания ПЭВМ должна иметь блокировку, которая обеспечивает отключение ее в случае остановки системы охлаждения и кондиционирования.

Воздуховоды также должны быть выполнены из негорючих материалов. Еще одним не маловажным дополнением для обеспечения пожарной безопасности является установление датчиков влажности, что препятствует предупреждению опасности коррозии, короткого замыкания.

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

4.4.1 Упражнения для глаз

При выполнении этого упражнения происходит эффект расслабления и укрепления глазных мышц, избавление от боли в глазах.

Необходимо закрыть глаза и расслабить мышцы лба, медленно с напряжением сместить глазные яблоки в крайне левое положение, через 1 минуту таким же способом перевести взгляд вправо. Это упражнение проделать 10 раз. Необходимо следить за тем, чтобы веки не подрагивали, и чтобы не щуриться.

При выполнении этого упражнения происходит химическое восстановление рецепторов глаз, а также расслабление глазных мышц, происходит процесс улучшения кровообращения в зрительном аппарате и происходит избавление от ощущения усталости глаз.

Необходимо: моргать в течении одной-двух минут, с помощью напряжения закрывать попеременно один глаз, а потом другой глаз на три-пять секунд, несколько раз в течении десяти секунд сильно зажмурить глаза, менять направление взгляда в течении десяти секунд: вправо, влево, вверх, вниз, прямо, тереть ладони одну о другую с такой силой, чтобы появилось ощущение тепла, после ощущения тепла необходимо закрыть глаза теплыми ладонями так, чтобы лучи света не поступали к глазам, скрестив при этом пальцы в центре лба, расс-

лабиться и дышать свободно и пробыть в таком положении две минуты, при этом на глаза и веки не нажимать.

4.4.2 Упражнения для головы и шеи

Эффект при выполнении данных упражнений: расслабление мышц шеи и лица, головы и плечевого пояса.

Для того, чтобы снять напряжение лицевых мышц нужно помассировать лицо. В течении десяти секунд надавливая пальцами на затылок сделать вращательные движения вправо, а затем влево. Закрыть глаза и сделать глубокий вход, на выходе медленно опустить подбородок и при этом расслабить шею и плечи. После снова глубоко вдохнуть, сделать медленное круговое движение головой влево и выдохнуть. Проделать эти упражнения три раза вправо, а затем три раза влево.

4.4.3 Упражнения для рук

После выполнения этих упражнений получается эффект снятия напряжения в кистях и запястьях, избавление от усталости рук.

В положении сидя или стоя разместить руки перед лицом, ладони наружу, пальцы выпрямлены, а после напрячь ладони и запястья. Собрать пальцы в кулаки, при этом быстро загибая их один за другим (начать нужно с мизинцев), после чего большие пальцы окажутся сверху. Сжатые кулаки повернуть так, чтобы они «посмотрели» друг на друга, движение должны происходит только в запястье, а локти должны быть не подвижны. Далее разжать кулаки и расслабить кисти, и проделать это упражнение несколько раз. В положении сидя или стоя опустить руки вдоль тела, расслабить их, сделать глубокий вдох и при медленном выдохе слегка потрясти руками в течении пятнадцати секунд и проделать это упражнение несколько раз. Для следующего упражнения сцепить пальцы, соединить ладони, приподнять локти, далее поворачивать кисти пальцами внутрь (к груди), то наружу и так проделать несколько раз, а после опустить руки и потрясти расслабленными кистями. Широко расставить пальцы и напрячь кисти секунд на семь, далее сильно сжать пальцы в кулаки, после чего

разжать кулаки, потрясти расслабленными кистями.

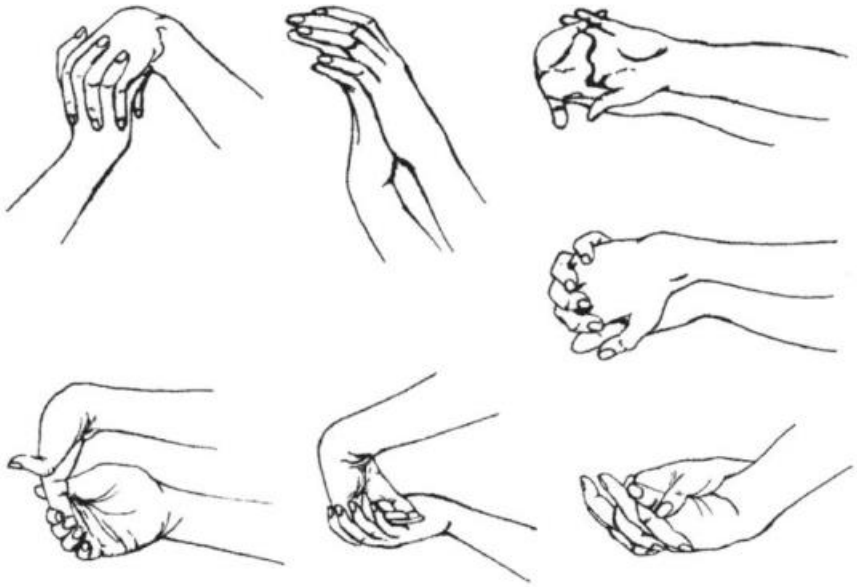

Рисунок 30 – Упражнения для пальцев и кистей рук

4.4.4 Упражнения для туловища

После выполнения этих упражнений работник сможет ощутить расслабление мышц, выпрямление позвоночника и улучшение кровообращения.

Необходимо встать прямо, расставить ноги на ширине плеч, руки поднять вверх и подняться на носочки и потянуться, опуститься и руки опустить вдоль туловища, проделать три раза. Поднять плечи, как только это возможно и плавно отвести их назад, затем медленно выставить вперед, так сделать десять раз. Из позы стоя прямо нагнуться и приложить ладони к ногам сзади колен, втянуть живот и при этом напрячь спину, после выпрямиться и расслабиться. Для следующего упражнения встать прямо и ноги на ширине плеч, развести руки в стороны на уровне плеч, на сколько это возможно повернуть туловище вправо и влево, проделать упражнение десять раз. Нужно сеть удобно на стул, вытянуть правую ногу вперед и согнуть ее в колене, и потянуть к груди, затем вытянуть ее обратно, после опустить ногу на пол и повторить это упражнение для левой ноги, для обеих ног.

ЗАКЛЮЧЕНИЕ

Целью исследования является повышение качества контроля за исполнением поручений.

В процессе выполнения данной работы проведен анализ организационной структуры ЦИТС и ЗИ, анализ информационной безопасности, анализ внешнего и внутреннего документооборота ЦИТС и ЗИ, согласно государственному стандарту, разработано техническое задание на создание информационной системы «контроль исполнения поручений».

Информационная система реализована при помощи СУБД MySQL и языка программирования C#.

Результатом проделанной работы является спроектированная информационная система «контроль исполнения поручений» для ЦИТС и ЗИ. Данная информационная система позволяет ознакомится с актуальными задачами, содержащимися в рабочем плане сотрудников, установить сроки исполнения задач, отслеживать исполнение, вносить изменения и комментарии к проделанной работе, а также эффективно управлять личным составом Центра.

В процессе проектирования информационной системы «контроль исполнения поручений» произведен анализ угроз информационной безопасности ЦИТС и ЗИ, произведена оценка безопасности и экологичности Центра.

По итогам проектирования информационной системы «контроль исполнения поручений» принято решение о внедрении данной информационной системы в общую ИСОД.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Комплексная система защиты информации на предприятии: учеб. пособие для студ. высш. учеб. заведений /В.Г. Грибунин, В.В. Чудовский. – М.: Издательский центр «Академия», 2018. – 416 с. Бейли Л.М. Изучаем PHP и MySQL/ Л.М. Бейли. – М.: Эксмо, 2018. – 800 с.

2 Коцюба И.Ю., Чунаев А.В. – Основы проектирования информационных систем – Санкт-Петербург, 2016 – 145 с.Бенкен, Е.С. PHP, MySQL, XML: программирование для Интернета/ Е.С. Бенкен. – СПб: BHV, 2017. – 336 с.

3 Моругин С.Л. Проектирование информационных систем. Методические указания по выполнению курсового проекта для студентов специальности 230102 (071900) – Нижний Новгород, НГТУ – 2017.

4 Маклаков С.В. BPWin и ERWin. CASE-средства разработки информационных систем. – М.: ДИАЛОГ-МИФИ, 2020 – 256 с.

5 Семененко В.А. Информационная безопасность: Учебное пособие. 2-е С3О изд., стереот. – М.: МГИУ, 2019. – 215 с.

6 https://ru.wikipedia.org/wiki/ «Угрозы информационной безопасности» от 18.06.2021г.

7 Прохоров С.А., Федосеев А.А., Иващенко А.В. Автоматизация комплексного управления безопасностью предприятия / Самара: СНЦ РАН, 2018 – 55 с., ил.

8 Астахова, Л.В. Теория информационной безопасности и методология защиты информации: Конспект лекций. -Челябинск, 2021. -361 с

9 Информационная безопасность: нормативно-правовые аспекты: учеб. пособие по специальностям 090102 «Компьютерная безопасность», 090105 Ю. А. Родичев. – СПб. и др.: Питер, 2019. – 271 с.

10 Организационное обеспечение информационной безопасности учебник для высш. учеб. заведений по направлению «Информационная безопасность» / О.А. Романов, С.А. Бабин, С.Г. Жданов. – Ю.М.: Академия, 2021.

- 188 с.

11 Акулов О.А. Информатика: базовый курс: учебник / О.А. Акулов, Н.В. Медведев. – 4-е изд., стер. – М.: Омега-Л, 2021. – 560 с.

12 Анин Б.Ю. Защита компьютерной информации. – БХВ-Петербург, 2020. – 384 с.

13 Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. — М.: Академический Проект; Гаудеамус,2018. – 544 с.

14 Информатика: учеб. пособие / С.М. Патрушина [и др.]; под ред. С.М. Патрушиной. – Изд. 2-е, перераб. и доп. – М.: МарТ; Ростов н/Д.: МарТ, 2019. – 400 с.

15 Куприянов, А.И. Основы защиты информации: учеб. пособие по специальностям «Радиоэлектрон. Системы», «Средства радиоэлектрон. борьбы» и «Информ. системы и технологии» / А.И. Куприянов, А.В. Сахаров, В.А. Шевцов Ю.М.: Академия, 2018. – 253 с.

16 Правовое обеспечение информационной безопасности: учеб. пособие /под ред. С.Я. Казанцева. – 2-е изд., испр. и доп. – М.: Академия, 2020. – 238 с.

17 Коноплева, И. А. Управление безопасностью и безопасность бизнеса: учеб. пособие по специальности «Прикладная информатика (по обл.)»/ И. А. Коноплева, И. А. Богданов. – М.: ИНФРА-М, 2017. – 446.

18 Пособие по безопасной работе на персональных компьютерах/ разраб. В.К. Шумилин. – М.: НЦ ЭНАС, 20017. – 28 с.

19 Шумилин, В.К. ПЭВМ. Защита пользователя [Текст] / Шумилин В.К. – М. : Охрана труда и социальное страхование, 2020. – 214с.

20 Кардаш, Т.А. Эргономика рабочих мест служащих и инженерно-технических работников, оснащенных ПЭВМ [Текст]: учеб. пособие /

21 Т.А. Кардаш; АмГУ, ИФФ. – Благовещенск: Изд-во Амур. гос. ун-та, 2018. – 60 с.

ПРИЛОЖЕНИЕ А

Техническое задание

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Полное наименование системы и ее условное обозначение

Полное наименование разрабатываемой информационной системы – информационная система «Контроль исполнения поручений» для УМВД России по Амурской области, Центр информационных технологий, связи и защиты информации (далее ЦИТСиЗИ).

Условное обозначение – «Контроль исполнения поручений»

1.2 Наименование предприятия разработчика, заказчика, их реквизиты

Заказчик информационной системы – кафедра информационных и управляющих систем, факультета математики и информатики Амурского государственного университета.

Реквизиты предприятия – заказчика:

1 Юридический адрес – 675027, г. Благовещенск, ул. Игнатьевское шоссе, 21

2 Телефон – 8 (4162) 39-45-25

3 E-mail – master@amursu.ru

4 Официальный сайт – www.amursu.ru

Разработчиком системы является студентка факультета математики и информатики, кафедры информационных и управляющих систем Амурского государственного университета Бакланова Тамара Николаевна.

1.3 Перечень документов, на основании которых создается система

Основанием для проектирования системы послужили следующие документы:

- заявка на разработку информационной системы;

- приказ УМВД России по Амурской области, ЦИТСиЗИ редакция от 7

мая 2021 года;

– приказ о типовой организационной структуре;

– должностные инструкции сотрудников организации;

– первичные документы;

– ГОСТ 34.602-89 Техническое задание на проектирование автоматизированной системы управления.

1.4 Плановые сроки начала и окончания разработки системы

Плановые сроки начала и окончания работ по созданию системы: начало разработки -февраль 2021 г., окончание – июнь 2021 г.

2 НАЗНАЧЕНИЕ И ЦЕЛИ СОЗДАНИЯ СИСТЕМЫ

2.1 Вид автоматизированной деятельности

Проектируемая система создается с целью контроля исполнения поручений сотрудниками Центра информационных технологий, связи и защиты информации, а также для автоматизации процесса решения задач, решение задач в сжатые сроки, контроль за их выполнением, возможность корректировки. Помимо значительного увеличения скорости осуществление контроля за исполнением поручений, система позволит исключить человеческий фактор, что уменьшит вероятность появления ошибки и значительно повысит надежность системы.

Текущее состояние процессов обработки и передачи необходимых документов Центра является трудоемким процессом, который подразумевает обработку больших массивов задач, а также многократный анализ схожих по структуре документов. Это приводит к значительным затратам времени, утомлению сотрудников и неточностям, допускаемым в силу усталости человека от монотонной деятельности. После внедрения системы значительная часть данных о предстоящем выполнении задач и рабочих графиках сотрудников будет возложена на ЭВМ, что позволит повысить эффективность работы сотрудников.

2.2 Перечень объектов, на которых предполагается использовать систему

Разрабатываемая система предназначена для контроля исполнения поручений и автоматизации постановки задач сотрудникам Центра.

2.3 Цели создания подсистемы

Целью создания системы является автоматизация постановки задач сотрудникам Центра. На данный момент все полученные задачи, оформление календарных планов, графиков работы сотрудников осуществляются вручную на бумажных носителях. Это приводит к значительным затратам времени и утомлению сотрудников и снижению качества выполнения задач. Внедрение системы позволит достаточно сократить время, затрачиваемое на обработку большого количества информации, быстро находить необходимые данные и с меньшими затратами выполнять необходимые задачи.

Основные цели проектирования:

– создание информационной системы;

– существенное сокращение трудоемкости и времени выполнения основных операций контролю за исполнением поручений;

– значительное сокращение времени обработки документации;

– возможность оперативного анализа хранящейся в базе данных информации по различным критериям и формирование результирующих отчетных документов;

– надежное хранение данных и защита от несанкционированного доступа;

– исключение дублирования информации при ее хранении;

– уменьшение временных затрат на обработку данных и повышение достоверности получаемой информации за счет автоматизированного сбора и хранения данных;

– формирование различных видов отчетов;

Продолжение приложения А

3 ХАРАКТЕРИСТИКА ОБЪЕКТА АВТОМАТИЗАЦИИ

3.1 Краткие сведения об объекте автоматизации

Центр информационных технологий, связи и защиты информации УМВД России по Амурской области, именуемое в дальнейшем ЦИТСиЗИ, создан в соответствии с Приказом МВД России, от 19 марта 2013 года N 169 Об утверждении Положения о Центре информационных технологий, связи и защиты информации Главного управления Министерства внутренних дел Российской Федерации.

ЦИТСиЗИ состоит отдела программирования, отдела информационных технологий, отдела криптографии и отдела специальной связи.

ЦИТСиЗИ работает около 16 сотрудников (руководитель ЦИТСиЗИ, инженеры 1, 2, 3 категорий, ведущий инженер и инженер отдела специальной связи).

ЦИТСиЗИ занимается выполнением следующих функций:

ЦИТСиЗИ расположены помещения для проведения специальной проверки оборудования, секретной обработки информации, настройки аппаратуры и её перепрограммирования.

В Центре используется новейшее специализированное оборудование.

Все вышеперечисленные виды деятельности осуществляются в соответствии с действующим законодательством РФ.

Основной целью деятельности Центра является обеспечение информационной безопасности.

Реквизиты компании: РОССИЯ, Амурская область, город Благовещенск, ул. 50 лет Октября, 18. ИНН 2801030145 ОГРН 1022800001377. тел.: 74162497830

3.2 Сведения об условиях эксплуатации и о характеристиках окружающей среды

Условия эксплуатации «Контроль исполнения поручений», диктуется

возможностями и рамками «Заказчика».

Элементы «Контроль исполнения поручений», функционируют в следующих климатических условиях 4 категории по ГОСТ 15150-69 (в помещениях (объемах) с искусственно регулируемыми климатическими условиями, например, в закрытых отапливаемых или охлаждаемых и вентилируемых производственных и других, в том числе хорошо вентилируемых подземных помещениях (отсутствие воздействия прямого солнечного излучения, атмосферных осадков, ветра, песка и пыли наружного воздуха; отсутствие или существенное уменьшение воздействия рассеянного солнечного излучения и конденсации влаги), исключение составляют каналы связи с удаленными объектами.

Характеристики окружающей среды:

1 температура окружающего воздуха в пределах 20 ± 10 °С;

2 относительная влажность окружающего воздуха в пределах 70 ± 15 %;

3 атмосферное давление в пределах 84-107 КПа.

4 ТРЕБОВАНИЯ К СИСТЕМЕ

4.1 Требования к системе в целом

4.1.1 Требования к структуре и функционированию системы

4.1.1.1 Перечень систем, их назначение и основные характеристики, требования к числу уровней иерархии и степени централизации системы.

Проектируемая система будет представлена следующими системами:

– система ввода данных, представлена понятным для восприятия и удобным для работы интерфейсом, характеризуется наличием пиктограмм для наиболее часто используемых функций, а также содержащим удобные и понятные меню, что значительно упрощает работу и сокращает сроки обучения использованию данной системы;

– система обработки данных, представляет программные системы, которые состоят из функций и процедур. В начале процесса обработки данных система проверяет соответствие типов входных данных соответствующим типам

полей. Если обнаруживается несоответствие, то программа завершает процесс обработки и выдает сообщение об ошибке. Если несоответствия не обнаруживается, то процесс обработки происходит успешно.

– система хранения данных, представляется в виде физических таблиц данных, которые будут получены после выполнения всех этапов проектирования базы данных (изучение предметной области, инфологическое, логическое и физическое проектирование), а затем будут реализованы в СУБД.

– система вывода данных, представляется в виде выводимой отчётности, генерируемой по различным критериям на основании хранимых и некоторых промежуточных данных.

– система оформления документов, представлена формами шаблонов документов, что упрощает и ускоряет работу их оформления.

– система удаления данных, представлена процедурами и функциями, которые на основании заданных сроков удаляют устаревшую и ненужную информацию.

– система обеспечения корректности данных, проверяет соответствие типов данных соответствующим типам полей. Если обнаруживается несоответствие, то программа завершает процесс обработки и выдает сообщение об ошибке.

– справочная система, представлена в виде справочника, позволяющая максимально быстро и эффективно освоить новый программный продукт, благодаря таким своим свойствам как наглядность и полнота.

4.1.2 Требования к персоналу

4.1.2.1 Требования к численности пользователей

Численность персонала «Контроль исполнения поручений» должна удовлетворять перечисленным ниже требованиям:

− быть достаточной для выполнения обязанностей по «Контроль исполнения поручений»;

− обеспечивать полную занятость персонала при выполнении обязанностей по эксплуатации «Контроль исполнения поручений».

4.1.2.2 Требования к квалификации пользователей

Пользователями системы могут выступать:

– квалифицированные пользователи с техническим образованием;

– администраторы баз данных;

– специалисты в области информационных технологий и вычислительной техники.

Все пользователи системы должны быть «уверенными пользователями» операционной среды Windows.

4.1.2.3 Требования к режиму работы персонала

Режим работы пользователей системы определяется режимом работы УМВД России по Амурской области, отелом ЦИТСиЗИ.

4.1.2.4 Требования к порядку подготовки персонала к работе

Порядок подготовки персонала должен включать в себя:

2 обучение персонала функциональным обязанностям согласно должностным инструкциям и эксплуатационной документации «Контроль исполнения поручений»;

3 обучение персонала правилам техники безопасности;

4 проведение экзаменов на квалификационную группу по электробезопасности не ниже II (для эксплуатационного персонала – не ниже III).

Персонал, обслуживающий «Контроль исполнения поручений», должен быть подготовлен к выполнению своих обязанностей в соответствии с должностными инструкциями и эксплуатационной документации.

Перед началом работы с системой, пользователи, не обладающие такими навыками, должны пройти соответствующие курсы.

4.1.3 Требования к показателям назначения системы. Программное обеспечение информационной системы должно устойчиво функционировать.

Необходимо иметь возможность ограничивать права пользователей при обращении к данным, с целью защиты информации от случайного искажения.

Система должна иметь дружественный интерфейс с пользователем.

Целевое назначение системы должно сохраняться на протяжении всего срока эксплуатации системы.

4.1.4 Требования надежности

Показатели надежности для системы должны определяться действующими общими техническими требованиями по надежности информационных систем. Надежность создаваемой информационной системы обеспечивается:

– созданием отказоустойчивой в целом системы;

– возможностью восстановления данных после сбоев;

– осуществлением журналирования работы всей системы;

– выбором отказоустойчивого оборудования и его структурным резервированием;

– использованием источников бесперебойного питания;

– выбором топологии локальной вычислительной сети, обеспечивающей защищенность от возможности вторжения из внешней информационной среды;

– резервным копированием информации.

4.1.5 Требования безопасности.

Разрабатываемая система должна обеспечивать:

– механизм проверки данных получаемых от объекта на достоверность;

– невозможность обхода системы разграничения доступа действиями, находящимися в рамках выбранной модели;

– безопасное хранение перерабатываемых данных;

– безопасную работу в режиме обмена данными;

– разграничения прав доступа пользователей к отдельным системам.

4.1.6 Требования к эргономике и технической эстетике.

Создаваемая система должна отвечать требованиям эргономики, то есть обеспечивать комфортную работу пользователя в среде самой системы. Система должна обеспечивать максимально возможную скорость ввода данных. Интерфейс с пользователем не должен вводить в заблуждение, его организация должна быть похожа на организацию интерфейса большинства программных продуктов (главное меню, панель управления, статусная строка, кнопки закрытия и свертывания). С эстетической точки зрения интерфейс системы должен быть максимально понятным (использование пиктограмм).

4.1.7 Требования к транспортабельности

Требования, предъявляемые к ИС «Контроль исполнения поручений» транспортабельности, не предъявляются.

4.1.8 Требования к эксплуатации, техническому обслуживанию (сопровождению), ремонту и хранения компонентов системы.

Устойчивая и надежная работа системы обеспечивается только при регулярном выполнении работ по техническому сопровождению системы, при поддержании в работоспособном состоянии комплекса аппаратных средств, а также при жестком соблюдении пользователями требований эксплуатационной документации и регламентов работы системы.

Регламент обслуживания определяется дополнительными документами, выпускаемыми организацией перед началом эксплуатации системы. При нарушении условий эксплуатации системы, заданных в эксплуатационной документации и регламентах работы, только пользователь несет ответственность за последствия таких нарушений.

Авторские права на программное обеспечение, на архитектуру системы и модели данных принадлежат разработчику и защищаются действующим законодательством.

4.1.9 Требования по сохранности информации при авариях

Специализированные программные средства администратора системы должны обеспечивать:

– возможность полного или частичного восстановления программы в результате возникновения сбойных ситуаций;

– наличие системы дублирования на резервные устройства хранения с по следующим восстановлением.

4.1.10 Требования к защите информации от несанкционированного доступа.

Должен осуществляться контроль за процессами обработки информации, включая контроль за работой пользователей во всех режимах работы путем автоматического ведения системных журналов, в том числе, регистрацию попыток несанкционированного доступа, обнаруживаемых программными средствами защиты.

При этом должны выполняться следующие требования:

– система должна иметь защиту от несанкционированного копирования и переноса данных на другой компьютер

– должна осуществляться идентификация и аутентификация пользователей;

– для каждого пользователя необходимо назначать пароль (длиной не менее 6 символов) и права доступа к данным.

4.1.11 Требования к защите от влияния внешних воздействий

Компьютеры, на которых должна быть установлена ИС «Контроль исполнения поручений», должны находиться в специально оборудованных помещениях, в отдалении от отопительных приборов и электрических кабелей.

Компьютеры должны быть снабжены устройствами бесперебойного питания, для предохранения от перепадов напряжения и непредвиденного отключения электричества.

4.1.12 Требования к стандартизации и унификации

Продолжение приложения А

Разработка системы регламентируется следующими стандартами:

ГОСТ 34.602-89 Техническое задание на создание автоматизированной системы;

ГОСТ 7.1-2003 Библиографическое описание документа. Общие требования и правила составления;

ГОСТ 19.001-77 ЕСПД. Общие положения;

ГОСТ 19.004-80 ЕСПД. Термины и определения;

ГОСТ 19.101-77 ЕСПД. Виды программ и программных документов;

ГОСТ 19.102-77 ЕСПД. Стадии разработки;

ГОСТ 19.103-77 ЕСПД. Обозначение программ и программных документов;

ГОСТ 19.104-78 ЕСПД. Основные надписи;

ГОСТ 19.105-78 ЕСПД. Требования к программным документам, выполненным печатным способом;

ГОСТ 19.402-78 ЕСПД. Описание программы;

ГОСТ 19.502-78 Описание применения. Требования к содержанию и оформлению;

ГОСТ 19.505-79 Руководство оператора. Требования к содержанию и оформлению;

ГОСТ 19.508-79 Руководство по техническому обслуживанию. Требования к содержанию и оформлению;

ГОСТ 24.301-80 Общие требования к выполнению текстовых документов;

ГОСТ 34.201-89 Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем;

ГОСТ 34.601-90 Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания;

ГОСТ 34.602-89 Информационная технология. Автоматизированные системы. Техническое задание на создание автоматизированной системы;

ГОСТ 34.603-92 Информационная технология. Виды испытаний автоматизированных систем.

4.1.13 Требования к безопасности жизнедеятельности и охране окружающей среде

Разрабатываемая система должна отвечать всем требованиям, предъявляемым инструкциями по технике безопасности в организации. То есть для всего компьютерного оборудования должен быть предусмотрен заземляющий контур, все провода должны быть с неповрежденной изоляцией, рабочие станции и другое сетевое оборудование не должно превышать допустимый уровень шума 75 дБ), все мониторы должны удовлетворять нормам по электромагнитному излучению ТСО 03.

4.2 Требования к функциям

4.2.1 Перечень функций, подлежащих автоматизации

Информационная система должна состоять из следующих функциональных частей:

1 ввод данных – предоставляет понятный для восприятия и удобный пользовательский интерфейс, который позволяет вводить данные посредством экранных форм, что значительно упрощает работу и сокращает сроки обучения использования данной системы. Интерфейс базы данных должен обеспечивать ввод новых и изменение хранящихся данных в нужном формате. При вводе данных система должна проверять соответствие данных типам полей.

2 система вывода данных – автоматически формирует необходимые отчеты.

Система необходима для вывода следующих данных: список сотрудников, список задач.

3 система хранения информации – представляет собой физические таб-

лицы, которые будут получены после выполнения всех этапов проектирования базы данных. К этапам проектирования относится изучение предметной области, инфологическое, логическое и физическое проектирование. Затем данные таблицы должны быть реализованы в СУБД.

Система необходима для хранения: рабочих графиков сотрудников, данных о поставленных задачах, данные о дате и времени приема сотрудников на службу, данные о сотрудниках Центра.

4 запросная система – осуществляет автоматический поиск данных в базе по одному параметру и предоставляет найденные варианты пользователю.

5 система аутентификации пользователя – обеспечивает контроль доступа к системе пользователей. При входе в программу запускается система аутентификации и идентификации пользователя, что обеспечивает контроль доступа к системе пользователей. После ввода имени пользователя и пароля проверяется наличие записи о пользователе с такими реквизитами в базе данных. В случае неверного ввода имени и пароля доступ к программе закрывается для данного пользователя. Если же имя и пароль введены, верно, то осуществляется вход в программу и открывается главное меню программы.

6 система администрирования – система позволяет выполнять следующие функции:

– настройка соединения с сервером СУБД;

– защита системы от несанкционированного использования;

– архивирование, резервное копирование базы данных, настройка автоматического резервирования;

– восстановление базы данных.

7 справочная система, представленная в виде справочника, позволяющая максимально быстро и эффективно освоить новый программный продукт, благодаря таким своим свойствам как наглядность и полнота.

4.2.2 Временной регламент реализации каждой функции.

Временной регламент реализации каждой функций зависит от объема выборки, что характеризует возможность издержки времени.

4.2.3 Требования к качеству реализации функции

Качество реализации функций ИС «Контроль исполнения поручений» должно обеспечивать безотказную работу ИС «Контроль исполнения поручений».

4.2.4 Перечень и критерий отказов

Отказ возможен, произойти тогда, когда пользователи вводят некорректные данные в поля системы.

4.3 Требования к видам обеспечения

4.3.1 Организационное обеспечение

Для работы с информационной системой необходимо:

1 создать специальную литературу: руководство пользователя, руководство администратора;

2 внести изменения в организационную документацию;

3 провести инструктаж сотрудников ЦИТСиЗИ.

Особые требования предъявляются руководству пользователя, которое содержит не только основы работы с системой, но и описание возможных ошибок и конфликтных ситуаций. В нем также описана последовательность работ, необходимых для решения конкретных задач.

После ввода в действие информационной системы в Центре потребуется внесение соответствующих изменений в должностные инструкции сотрудников отдела, которые будут выполнять какие-либо работы с использованием этой системы.

4.3.2 Требования к информационному обеспечению

Требования к составу, структуре и способам организации данных в системе:

– наличие всех необходимых учетных атрибутов объекта автоматиза-

ции;

– независимость представления данных от СУБД.

Требования к информационной совместимости со смежными системами:

– полная автономность;

– независимость системы приема/отправки данных от изменения порядка признаков, их номенклатуры и способов хранения.

4.3.3 Требования к лингвистическому обеспечению

Вид обеспечения является совокупностью языковых средств, предназначенных для упрощения процесса общения пользователей с системой.

Состав лингвистического обеспечения включает в себя:

1 языки описания, управления и манипулирования данными в различных СУБД;

2 интерактивные системы взаимодействия пользователей с ЭВМ, к основным методам, организации диалогового взаимодействия которых относятся режим выбора функций и режим выполнения функций;

3 языковые средства систем автоматизации проектирования, включая алгоритмические языки и специализированные языки;

В качестве СУБД в системе используется СУБД SQL Server, которая отвечает всем необходимым требованиям, а именно:

1 реализация архитектуры «клиент-сервер», так как это значительно упростит клиентские приложения (все работы по обслуживанию БД будет выполнять сервер БД);

2 осуществление работы с данными по средствам языка структурированных запросов SQL, что приведет к снижению сетевого трафика;

3 наличие необходимых средств для распределения прав доступа, так как это упростит администрирование БД и повысит ее защищенность.

Требования по лингвистическому обеспечению предполагают использование единого логического и понятийного интерфейса для пользователей.

4.3.4 Требования к программному обеспечению

Для клиентских мест необходимо использовать приложение, позволяющее вносить информацию в базу данных и заполнять формы отчетов. Должна быть возможность добавлять данные в базу посредствам экранных форм, интуитивно понятных пользователю системы. Такой подход облегчает и упрощает выполнение процесса документооборота, для сотрудников регистратуры, а также исключает возможные ошибки оформления.

Сотрудники регистратуры могут получать различные отчеты. Поскольку необходимо обеспечить защиту информационной системы от несанкционированного доступа, то каждый сотрудник имеет свой пароль для входа в систему, обеспечивающий ввод и редактирование только данных согласно своему уровню доступа.

Формы приложения должны иметь простой, интуитивно понятный даже неопытному пользователю интерфейс. Главное требование к приложению – понятная формулировка задачи, предполагающее однозначный ответ.

Реализацию информационной системы в дальнейшем предполагается осуществить посредством использования следующих программных продуктов:

– средство построения модели информационных потоков организации BPWin;

– средство разработки структуры базы данных ERWin;

– СУБД SQL Server;

– язык программирования C#;

BPWin – мощный инструмент моделирования с возможностью анализа, документирования и корректирования бизнес процессов. Он поможет устранить лишние или неэффективные операции, уменьшить издержки, повысить гибкость и улучшить уровень обслуживания заказчика.

В модели BPWin существует возможность четко задокументировать важ-

ные позиции, такие как необходимые операции, проследить, как они выполняются и какие необходимы для этого ресурсы. Модель BPWin обеспечивает интегрированное изображение того, как работает организация. Это изображение, в свою очередь, состоит из подмоделей отделов.

BPWin включает несколько расширений, поддерживающих методологии моделирования IDEF0, DFD и IDEF3. BPWin поддерживает двунаправленные линии связи с программой ERWin.

ERWin – средство концептуального моделирования БД, использующее методологию IDEF1X. ERwin реализует проектирование схемы БД, генерацию ее описания на языке целевой СУБД (ORACLE, Informix, Sybase, DB/2, Microsoft SQL Server, Progress) и реинжиниринг существующей БД. ERwin выпускается в нескольких различных конфигурациях, ориентированных на наиболее распространенные средства разработки приложений 4GL. Для ряда средств разработки приложений (SQLWindows, Delphi, Visual Basic) выполняется генерация форм и прототипов приложений.

C# («Си Шарп») – один из наиболее быстро растущих, востребованных и при этом «удобных» языков программирования. Это модификация фундаментального языка C от компании Microsoft, призванная создать наиболее универсальное средство для разработки программного обеспечения для большого количества устройств и операционных систем. C# – современный объектно-ориентированный и типобезопасный язык программирования. C# позволяет разработчикам создавать множество типов безопасных и надежных приложений, работающих в экосистеме .NET. C# относится к широко известному семейству языков C, C++, Java или JavaScript.

C# позволяет динамически выделять объекты и хранить упрощенные структуры в стеке. C# поддерживает универсальные методы и типы, обеспечивающие повышенную безопасность типов и производительность. C# предоставляет итераторы, которые позволяют разработчикам классов коллекций опреде-

лять пользовательские варианты поведения для клиентского кода.

В C# особое внимание уделяется управлению версиями для обеспечения совместимости программ и библиотек при их изменении. Вопросы управления версиями существенно повлияли на такие аспекты разработки C#, как раздельные модификаторы virtual и override, правила разрешения перегрузки методов и поддержка явного объявления членов интерфейса.

4.3.5 Требования к техническому обеспечению

Для реализации и эксплуатации программного обеспечения пользователь должен иметь установленную операционную систему семейства Windows.

Минимальные требования для работы на персональных компьютерах, имеющих следующие минимальные характеристики:

– тактовая частота процессора – 2.0 ГГц;
– ОЗУ – 4 ГБ или более
– на жестком диске при установке используется около 100 Мбайт;
– объем жесткого диска зависит от объема БД.

Данные характеристики были выбраны для эффективной работы без ожидания отклика системы на запросы персонала, а также обеспечения целостности, сохранности информации при сбоях различного характера.

Требования к рабочим станциям должны быть минимальны, обеспечивающих функционирование системы без сбоев из-за переполнения ресурсов:

1 монитор;
2 модем;
3 принтер;
4 устройства ввода информации – клавиатура, мышь;
5 сетевая карта Fast Ethernet 100-TX Мбит/с.

5 СОСТАВ И СОДЕРЖАНИЕ РАБОТ ПО СОЗДАНИЮ СИСТЕМЫ

5.1 Перечень этапов работ по созданию системы

Стадии и этапы разработки:

– исследование предметной области, анализ процессов деятельности предприятия, выделение объекта автоматизации;

– составление технического задания: выяснение требований заказчика к разрабатываемой системе, определение технических и программных средств, необходимых для реализации проекта, уточнение функций системы;

– составление эскизного проекта (разработка предварительных проектных решений, разработка документации на систему);

– составление технического проекта (разработка проектных решений по системе, разработка и тестирование отдельных модулей системы);

– программная реализация информационной системы;

– рассмотрение существующей структуры сети и ее возможная модернизация;

– согласование созданной информационной системы с требованиями заказчика, учет всех полученных замечаний и указаний;

– составление необходимой документации по эксплуатации и сопровождению системы и предоставление её заказчику;

– внедрение и сопровождение системы: установка и настройка программно-аппаратных средств, обучение пользователей работе с системой, ознакомление администратора с его обязанностями по сопровождению системы, выявление и устранение неполадок.

5.2 Сроки выполнения

Сроки выполнения каждой функции варьируется от 2 до 7 дней, в зависимости от объема перерабатываемой информации.

5.3 Исполнители работ

Исполнителем работ является студент группы 755 Амурского государственного университета, факультета математики и информатики, кафедры информационных и управляющих систем – Бакланова Тамара Николаевна.

Продолжение приложения А

6 ПОРЯДОК КОНТРОЛЯ И ПРИЁМКИ СИСТЕМЫ

Отработка оптимальных форм организации работ по эффективной эксплуатации системы производится в ходе её опытной эксплуатации. Результаты испытаний оформляются в виде проекта и используются при разработке эксплуатационной документации и регламентов работы с системой.

Испытания ИС «Контроль исполнения поручений» проводятся «Заказчиком» в согласованные сроки.

Испытания проводятся специально создаваемой Комиссией кафедрой информационных технологий, в которую включаются представители «Исполнитель» и «Заказчик».

7 ТРЕБОВАНИЯ К СОСТАВУ И СОДЕРЖАНИЮ РАБОТ ПО ПОДГОТОВКЕ ОБЪЕКТА АВТОМАТИЗАЦИИ К ВВОДУ СИСТЕМЫ В ДЕЙСТВИЕ

Основные мероприятия, необходимые для ввода системы в действие:

– приведение поступающей в систему информации (в соответствии с требованиями к информационному и лингвистическому обеспечению). Исполнителем данного мероприятия является разработчик ИП «Контроль исполнения поручений»;

– создание условий функционирования проекта, при которых гарантируется соответствие создаваемой системы требованиям, содержащимся в ТЗ. Исполнителем данного мероприятия должен быть заказчик;

– сроки обучения персонала работе с новой системой определяется длительностью от одной до двух недель.

8 ТРЕБОВАНИЯ К ДОКУМЕНТИРОВАНИЮ

Состав и содержание документации должны соответствовать требованиям ГОСТ 34.201-89 и нормативно-технических документов (комплекса стандартов и руководящих документов на автоматизированные системы и единой системы программной документации).

Документация на проектируемую систему должна включать:

– рабочую документацию (на систему в целом, достаточную для ввода в действие, функционирования и обеспечения работоспособности системы);

– эксплуатационную документацию, предназначенную для использования при эксплуатации системы;

– документацию на программные средства вычислительной техники;

– техническое задание;

– эскизный проект;

– технический проект;

– сведения о тестировании подсистемы (включая тестовые данные).

8.1 Перечень подлежащих документов к разработке

Перечень документов, подлежащих разработке на систему: схема функциональной структуры; описание организации информационной базы; руководство по организации сопровождения; программа и методика испытаний; описание применения; технологическая инструкция.

8.2 Перечень документов на машинном носителе

Перечень документов, подлежащих разработке по каждому комплексу задач, входящих в разрабатываемую систему: описание постановки комплекса задач с перечнем выходных данных (документов); описание технологического процесса обработки данных; руководство пользователя.

9 ИСТОЧНИКИ РАЗРАБОТКИ

Основные источники разработки:

– Приказ МВД РФ от 20 июня 2012 г. N 615 «Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации»

– приказ УМВД России по Амурской области, ЦИТСиЗИ редакция от 10 апреля 2021 года;

– инструкция по охране труда при работе на компьютере;

– ГОСТ 34.602-89 – техническое задание на проектирование автоматизированной системы управления.

Приложение Б

Программный интерфейс

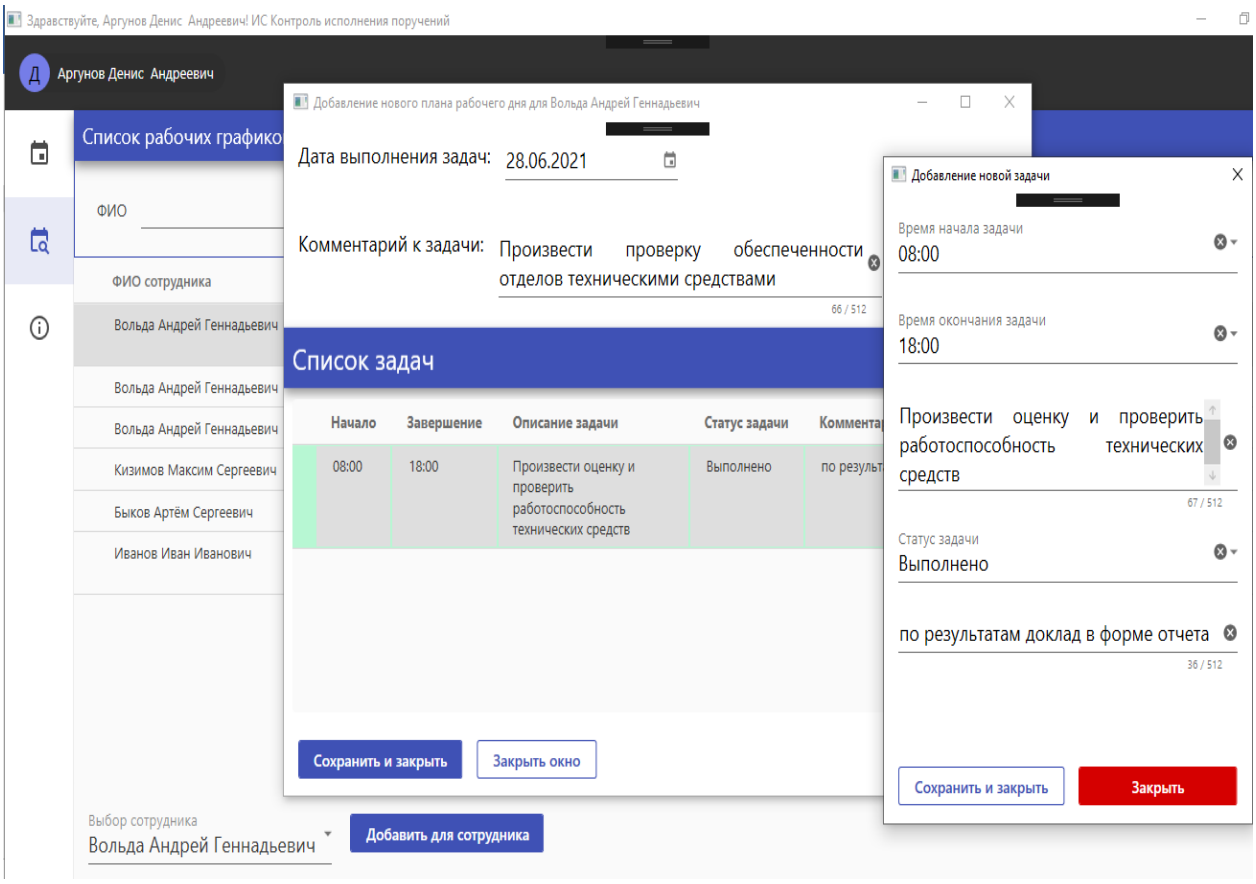

Рисунок 33 – Постановка задач сотрудникам Центра

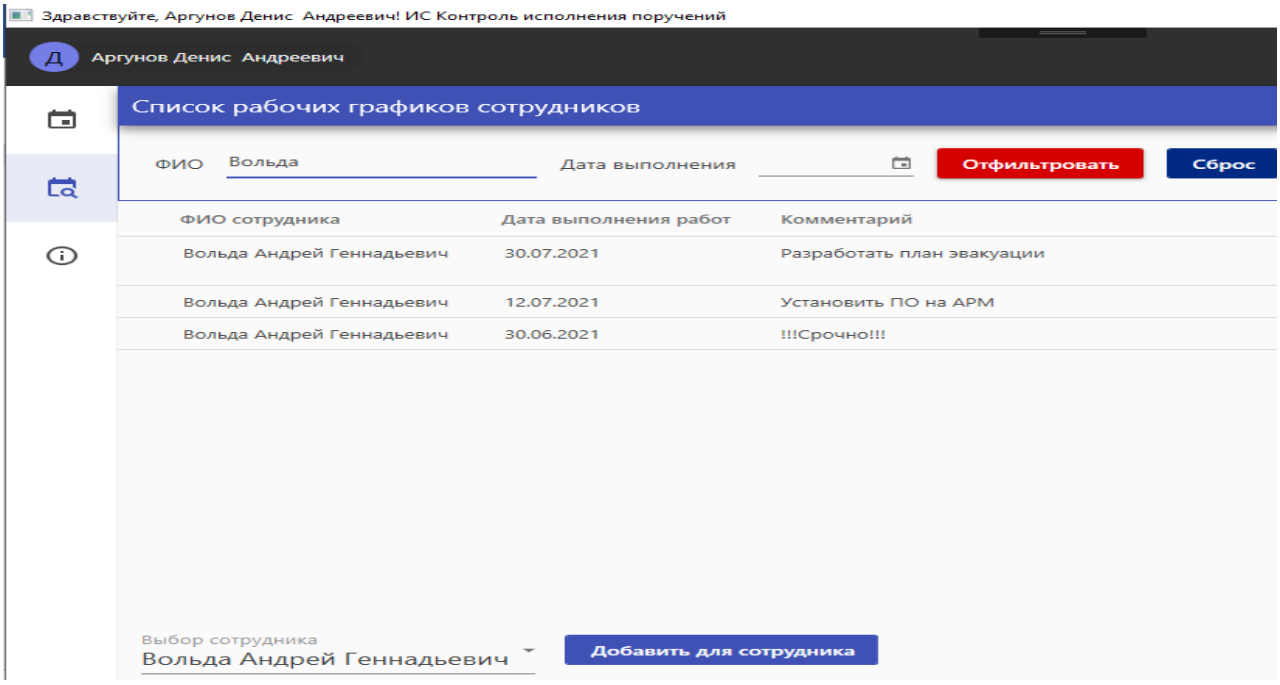

Рисунок 34 – Осуществление поиска графиков сотрудников

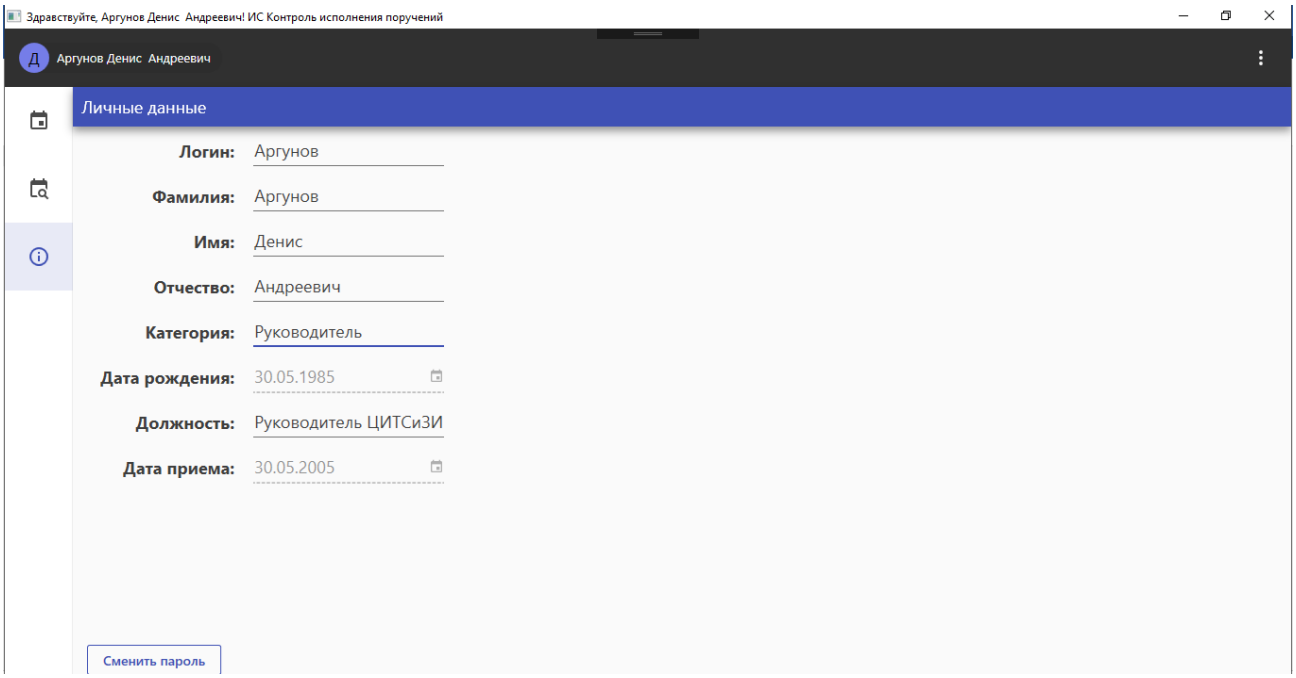

Рисунок 35 – Личные данные сотрудника

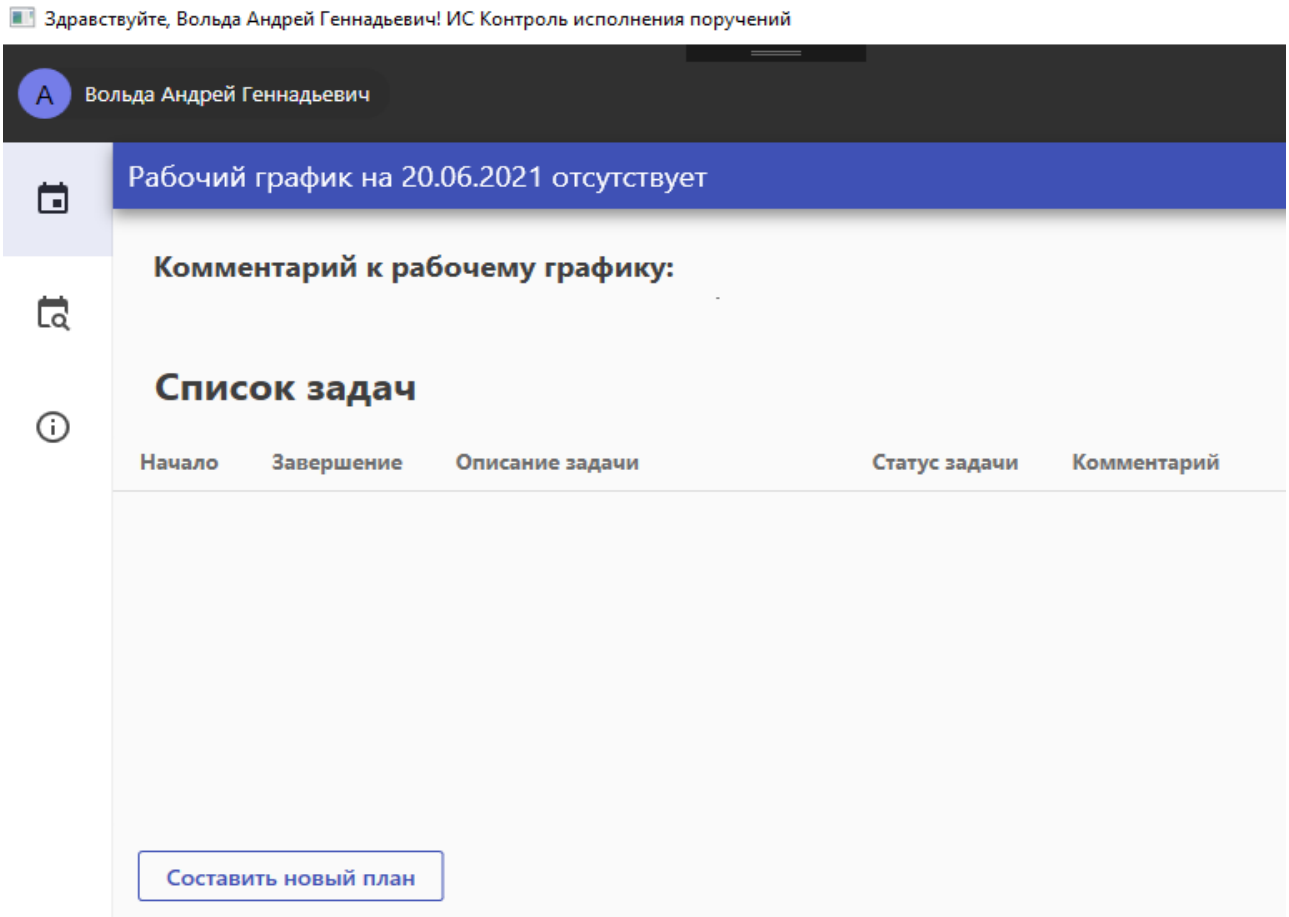

Рисунок 36 – Экранная форма начальника отдела

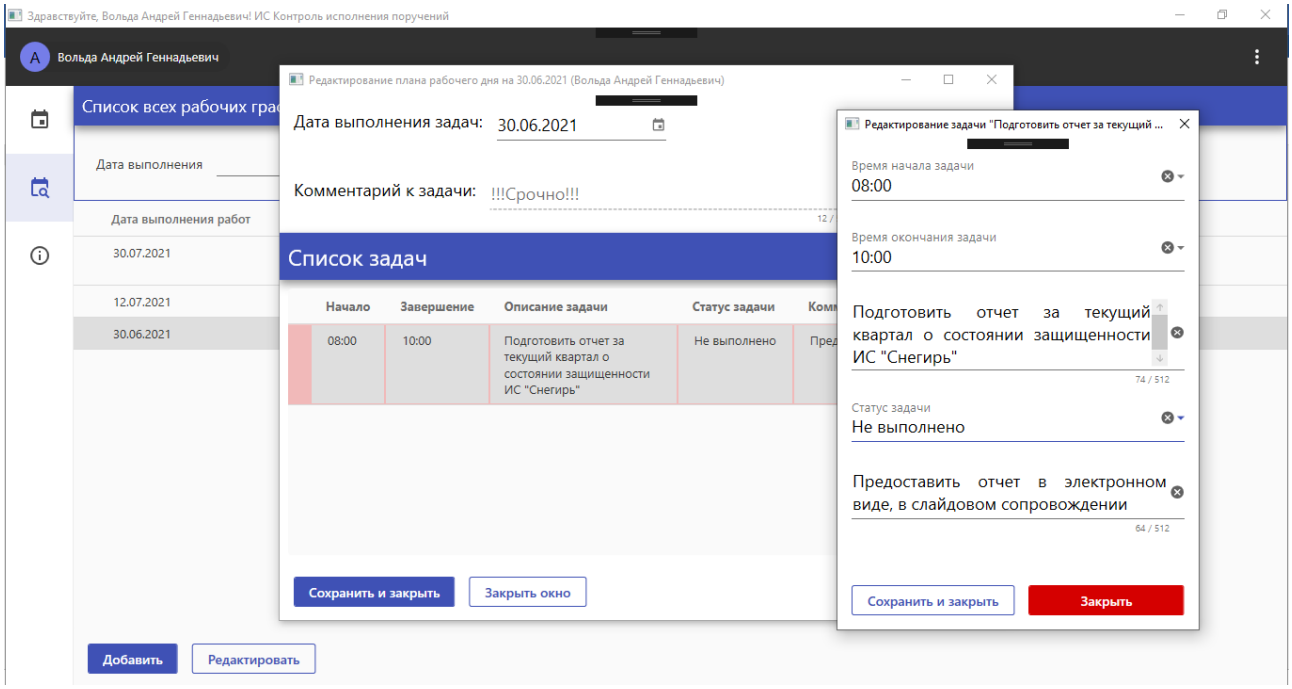

Рисунок 37 – Отчет о задаче, которая не была выполнена

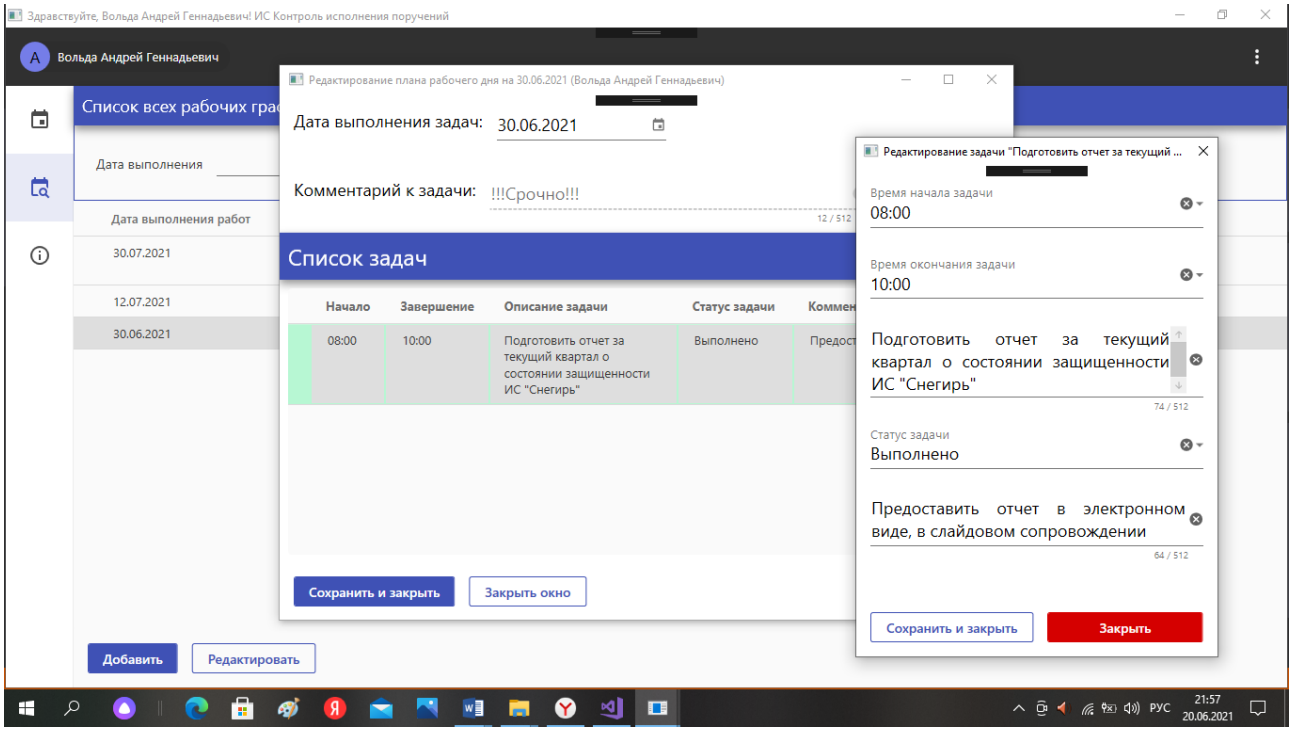

Рисунок 38 – Отчет о выполненной задаче